

УДК 657.6+658.01:004(036); 002:004.056; 65.012.8

№ держреєстрації 0112U007713

Інв. № _____

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
65026, м. Одеса, вул. Преображенська, 8, тел. (048) 23-61-58

ЗАТВЕРДЖУЮ

Ректор

Одеського національного
економічного університету
докт. екон. наук, професор

_____ *М.І. Звєряков*

«___» _____ 2014 р.

ЗВІТ

про науково-дослідну роботу

**УДОСКОНАЛЕННЯ ПРИНЦИПІВ ТА МЕТОДІВ
ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ,
ІНФОРМАЦІЙНОЇ ТА ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ
ПІДПРИЄМСТВ ТА ОРГАНІЗАЦІЙ
СФЕРИ ЕКОНОМІКИ, БІЗНЕСУ ТА ФІНАНСІВ**

(проміжний)

Рукопис закінчено 1 грудня 2014 року

Науковий керівник НДР

*завідувач кафедри Інформаційних систем в економ
докт. техн. наук, доцент*



О.О. Скопа

Одеса - 2014

СПИСОК ВИКОНАВЦІВ

Науковий керівник

докт. техн. наук, доцент

(вступ, підрозділи 2.1, 2.2, розділ 6, висновки до звіту)

О.О. Скопа

Відповідальний виконавець

канд. екон. наук, доцент

(підрозділи 1.2...1.5, висновки до розділів)

О.В. Орлик

Виконавці

канд. техн. наук, доцент

(підрозділи 2.2, 4.9, розділи 6-8)

Н.Ф. Казакова

канд. техн. наук, доцент

(підрозділи 1.6, 4.1-4.8, 5.4)

Ю.В. Щербина

канд. техн. наук, доцент

(підрозділи 2.2, 4.10)

С.Л. Волков

канд. техн. наук, доцент

(підрозділ 4.10)

О.В. Грабовський

канд. техн. наук, доцент

(розділ 9)

В.А. Лахно

канд. екон. наук, ст. викладач

(підрозділи 5.1, 5.6)

О.І. Мацків

ст. викладач

(підрозділи 5.7, 5.8)

О.Г. Єсіна

ст. викладач

(підрозділи 5.9, 5.10)

А.Ю. Вакула

ст. викладач

(підрозділи 3.1-3.3)

О.О. Фразе-Фразенко

викладач

(підрозділ 1.1)

О.О. Йона

аспірант

(підрозділи 2.1, 5.2)

Є.В. Вавілов

аспірант

(підрозділ 1.6)

К.Б. Айвазова

аспірант

(підрозділи 5.3, 5.5)

С.Д. Асабашвілі

У наукових дослідженнях кафедри прийняли участь 8 студентів ОНЕУ. Результати їх досліджень опубліковано у 8 статтях, а саме: Г. Васильченко [308], А.-М. Аль-Джамалі [309], М. Атанасов [310], О. Бандура [311], О. Янгьоз [312], Ю. Баланюк [313], Д. Осипенко [314], В. М. Буй [319].

РЕФЕРАТ

Звіт з НДР «Удосконалення принципів та методів інформаційного забезпечення, інформаційної та фінансово-економічної безпеки підприємств та організацій сфери економіки, бізнесу та фінансів» складається зі вступу, 9 розділів з висновками, загального висновку до роботи та списку використаних літературних джерел. Звіт викладено на 527 сторінках, містить 492 сторінки основного тексту з 104 таблицями та рисунками (з них 23 – на окремих сторінках) та списком використаних літературних джерел з 415 найменувань на 35 сторінках.

Предмет наукового дослідження

Інформаційне забезпечення, інформаційна та фінансово-економічна безпека підприємств та організацій сфери економіки, бізнесу та фінансів

Об'єкт наукового дослідження

Методологія удосконалення принципів та методів інформаційного забезпечення, інформаційної та фінансово-економічної безпеки підприємств та організацій сфери економіки, бізнесу та фінансів

Мета

Виконання теоретичних досліджень щодо удосконалення існуючих принципів та методів інформаційного забезпечення, інформаційної та фінансово-економічної безпеки підприємств та організацій сфери економіки, бізнесу та фінансів

Методи дослідження

- апарат методів експертних оцінок та експертних систем з метою аналізу та прогнозування ситуацій в галузі забезпечення інформаційної безпеки;

- з метою розробки комплексної інтегрованої технології оцінки якості функціонування ІВС та її оптимізації й управління протягом життєвого циклу та при вирішенні питань програмно-технічної та алгоритмічної реалізації пропонуванних методів, використовувалися елементи теорії чисел, методи комбінаторного аналізу та теорії кінцевих полів, елементи теорії нечітких множин та нечіткої логіки, методи багатокритеріальної та багатопараметричної оптимізації, методи кваліметрії, генетичні алгоритми, а також методи математичного та імітаційного моделювання;

- з метою розробки принципів аутентифікації у системах розпізнавання образів у банківських системах використовувалися теорія розпізнавання образів у якості базового засобу; математичні методи, включаючи теорію груп, кілець, полів та елементи математичного аналізу; методи статистичної обробки сигналів; елементи теорії топології; теорія прийняття рішень; методи об'єктно-орієнтованого програмування, програмні та мовні засоби сучасних комп'ютерних технологій.

Практична цінність

На основі результатів наукових досліджень, проведених на 1 етапі НДР, для навчального процесу кафедри визначено наступну практичну цінність отриманих результатів:

- удосконалено розділ «Інформаційна безпека» курсу лекцій з дисциплін «Інформаційні системи та технології УП та ЕП» напряму 6.030505 «Управління персоналом та економіка праці»;

- удосконалено розділ «Інформаційна безпека» курсу лекцій з дисциплін «Інформаційні системи та технології» напряму 6.140101 «Готельно-ресторанна справа»;

- удосконалено розділ «Інформаційна безпека» курсу лекцій з дисциплін «Інформаційні системи та технології в менеджменті» напряму 6.030601 «Менеджмент»;

- на розгляд кафедри внесено пропозиції щодо удосконалення існуючих та розробки нових практичних та лабораторних робіт для вище зазначених спеціальностей;

- матеріали, отримані та представлені у звіті, опубліковані у статтях у виданнях за переліками ВАК України, а також підготовлені до опублікування у монографії за темою дослідження. Вони можуть бути використані при підготовці фахівців спеціальності 8.18010014 «Управління фінансово-економічною безпекою» кваліфікації «Професіонал з фінансово-економічної безпеки» та «Аналітик з питань фінансово-економічної безпеки».

Новизна роботи

Розроблено та удосконалено методологію, методики, методи та засоби щодо збереження та захисту інтелектуальної власності, конфіденційної клієнтської інформації та іншої інформації, що має критично важливе значення для ведення бізнесу у вигляді стратегій або окремих рішень у сфері безпеки, які тісно ув'язані з цілями та завданнями бізнесу, а саме: управління ідентифікаційною інформацією і доступом; управління інформаційною та фінансово-економічною безпекою підприємств; конфіденційність та захист даних.

Область застосування

Організації та підприємства галузі економіки, бізнесу та фінансів

Ключові слова

Безпека, конфіденційність, доступність, управління, інформація, інформаційні технології, фінансово-економічна безпека, аутентифікація, розпізнавання

ЗМІСТ

	Стор.
РЕФЕРАТ	3
ВСТУП	13
<i>Підстави для проведення науково-дослідної роботи</i>	13
<i>Мета НДР</i>	18
<i>Основні завдання для досягнення мети</i>	18
<i>Взаємозв'язок з іншими роботами</i>	19
РОЗДІЛ 1 ФІНАНСОВО-ЕКОНОМІЧНА БЕЗПЕКА ПІДПРИЄМСТВ ТА ОРГАНІЗАЦІЙ СФЕРИ ЕКОНОМІКИ, БІЗНЕСУ ТА ФІНАНСІВ	20
1.1. Аналіз стану економічної безпеки у сфері економіки та бізнесу ..	20
1.2. Сутності комплексної системи забезпечення економічної безпеки підприємства	29
1.3. Система загроз економічній безпеці суб'єктів господарювання ...	38
1.4. Система управління фінансово-економічною безпекою підприємства	52
1.5. Множини систем економічної безпеки суб'єктів господарювання	57
1.6. Проблеми правового забезпечення захисту баз даних	62
<i>Висновки до розділу 1</i>	68
РОЗДІЛ 2 РОЗВИТОК ТЕОРІЇ ТА ПРАКТИКИ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ГАЛУЗІ ЕКОНОМІКИ, БІЗНЕСУ ТА ФІНАНСІВ	71
2.1. Інтелектуальні автономні системи галузі економіки, бізнесу та фінансів: концептуальні положення створення та функціонування	71
2.1.1. Цілеорієнтовна задача для галузі економіки, бізнесу та фінансів: передумови та вимоги	72
2.1.2. Елементи та проблеми концепції створення ІАС для галузі економіки, бізнесу та фінансів	73

2.2. Удосконалення методик, методів та засобів випробувань у телекомунікаційних мережах.....	85
2.2.1. <i>Задача скорочення обсягу профілактичних випробувань надійності об'єктів телекомунікаційних мереж.....</i>	85
2.2.2. <i>Процедура контрольних випробувань резервних систем на основі біноміальної схеми.....</i>	90
2.2.3. <i>Узгодження вимог до надійності та фінансування мереж зв'язку при проведенні профілактичних заходів .</i>	100
2.2.4. <i>Удосконалення елементів випробування надійності резервних каналів телекомунікаційних систем</i>	108
Висновки до розділу 2	122
РОЗДІЛ 3 КОНФІДЕНЦІЙНІСТЬ ТА ЗАХИСТ ДАНИХ	125
3.1. Синтез методики розрахунку коефіцієнтів помилкового пропуску та помилкової відмови доступу у системах біометричної ідентифікації	125
3.1.1. <i>Передумови та вибір методики розрахунку FAR та FRR.....</i>	127
3.1.2. <i>Визначення статистичних властивостей біометричних порівнянь</i>	129
3.1.3. <i>Методика розрахунку FAR та FRR.....</i>	132
3.1.4. <i>Обговорення результатів</i>	142
3.2. Аналіз сплайн-методів з метою їх застосування для обробки контурів зображень	149
3.3. Практична реалізація технології ідентифікації та оригінальності технічних засобів фіксації цифрових зображень	166
Висновки до розділу 3	171
РОЗДІЛ 4 ПРОБЛЕМИ ТА ЗАДАЧІ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ТА ДОСТОВІРНОСТІ ІНФОРМАЦІЇ.....	173
4.1. Задачі, що вирішуються криптографічними методами	177
4.2. Формалізація процесів у криптографічних системах.....	179
4.2.1. <i>Формальні моделі шифрів.....</i>	179
4.2.2. <i>Надмірність текстів.....</i>	182
4.2.3. <i>Математична модель текстів</i>	183
4.2.4. <i>Математичні критерії на відкритий текст</i>	190

4.3. Умови побудови досконалих шифрів	193
4.4. Параметри сучасних шифрів	197
4.5. Елементарні криптографічні перетворення	202
4.5.1. Підстановка – як основне криптографічне перетворення....	202
4.5.2. Математичні моделі шифрів заміни	204
4.5.3. Математичні моделі перестановочних шифрів	215
4.6. Загальні підходи до будування композиційних шифрів	217
4.7. Схема Фейстеля	225
4.8. Сучасні симетричні криптографічні системи	231
4.8.1. Загальні особливості побудови блочних симетричних криптографічних систем.....	232
4.8.2. Стандарт шифрування DES	234
4.9. Моделі розв’язання задачі про відновлення інформації	245
4.10. Технологія прогнозування ситуацій для систем з генетичними принципами функціонування	255
Висновки до розділу 4	260
РОЗДІЛ 5 СУЧАСНІ INTERNET-ТЕХНОЛОГІЇ: ОСНОВИ ПОБУДОВИ	261
5.1. Організація інформаційної взаємодії на мережному рівні моделі OSI	261
5.1.1 Архітектура Internet	262
5.1.2 Мережна адреса Internet	264
5.1.3 Протокол ARP	269
5.2 Протоколи ARP і RARP. Структура дейтаграми IP	272
5.2.1 Протокол RARP	274
5.2.2 Структура дейтаграми IP	276
5.3. Маршрутизація в мережах TCP/IP	280
5.3.1. Способи маршрутизації й доставки дейтаграм	281
5.3.2 Позакласові мережі TCP/IP	284
5.3.3 Алгоритм маршрутизації.....	287

5.4	Протокол ICMP.....	288
5.4.1	<i>Структура повідомлення ICMP.....</i>	288
5.4.2	<i>Повідомлення ICMP.....</i>	289
5.5	Протокол ICMP. Повідомлення REQUEST/REPLY	295
5.6	Протоколи маршрутизації. Алгоритм RIP	301
5.6.1	<i>Концепції логічної організації мереж.....</i>	301
5.6.2	<i>Концепція автономних систем.....</i>	303
5.6.3	<i>Типи протоколів маршрутизації.....</i>	305
5.6.4	<i>Алгоритм RIP.....</i>	306
5.7	Протокол маршрутизації OSPF	315
5.7.1	<i>Переваги використання протоколу OSPF.....</i>	315
5.7.2	<i>Основні компоненти й принципи організації інформаційного обміну</i>	317
5.8	Протоколи маршрутизації IGRP і EIGRP	325
5.8.1	<i>Протокол маршрутизації IGRP.....</i>	325
5.8.2	<i>Протокол маршрутизації EIGRP</i>	328
5.9	Протоколи зовнішньої маршрутизації	331
5.9.1	<i>Особливості зовнішньої маршрутизації.....</i>	331
5.9.2	<i>Протокол маршрутизації EGP.....</i>	332
5.9.3	<i>Протокол маршрутизації BGP.....</i>	335
5.10	Призначення й основні різновиди протоколів транспортного рівня.....	339
5.10.1	<i>Ідентифікація процесів на транспортному рівні.....</i>	340
5.10.2	<i>Транспортний протокол UDP</i>	340
5.10.3	<i>Транспортний протокол TCP</i>	342
	Висновки до розділу 5.....	348
	РОЗДІЛ 6 РОЗРОБКА МЕТОДІВ АПАРАТНО-ПРОГРАМНОГО УДОСКОНАЛЕННЯ ТЕХНОЛОГІЙ ЗАХИСТУ ІНФОРМАЦІЇ В ІНТЕГРОВАНИХ КОГНІТИВНИХ МЕРЕЖАХ В УМОВАХ ЕЛЕКТРОННОЇ ПРОТИДІЇ	350
6.1.	Забезпечення функціонування EF MISI в когнітивній мережі в умовах радіоелектронної протидії	353

6.1.1.	<i>Передумови забезпечення енергетичної скритності сигналів при передаванні конфіденційної інформації у радіоструктурах когнітивної мережі</i>	353
6.1.2.	<i>Вибір методу модуляції на основі широкосмугових хаотичних сигналів.....</i>	356
6.1.3.	<i>Імітаційне моделювання енергетичної скритності сигналів</i>	358
6.2.	<i>Розробка нового методу передавання конфіденційних даних у каналах Cross-П РС з обмеженою смугою</i>	362
6.2.1.	<i>Передумови проблеми передавання даних у каналах Cross-П РС.....</i>	362
6.2.2.	<i>Аналіз та опис структури спектру сигналу для Cross-П РС виділеної когнітивної мережі</i>	364
6.2.3.	<i>Розробка структури спектру для передавання низькошвидкісних потоків від систем управління СЗІ.....</i>	366
6.2.4.	<i>Технічне рішення задачі зменшення взаємних шумів у каналах управління системами захисту інформації</i>	366
6.3.	<i>Розробка безпечного передавального тракту для Cross-П РС з обмеженою смугою</i>	369
6.3.1.	<i>Передумови проблеми розробки передавального тракту для Cross-П РС когнітивної мережі</i>	369
6.3.2.	<i>Розробки структурної схеми передавального тракту для Cross-П РС.....</i>	370
6.3.3.	<i>Опис функціонування передавального тракту для Cross-П РС когнітивної мережі</i>	373
6.4.	<i>Розробка цифрового прецизійного часового дискримінатора для синхронізації технологічних процесів когнітивної мережі та процесів функціонування EF MISI</i>	375
6.5.	<i>Результати моделювання та експериментальних досліджень щодо функціонування елементів СЗІ Cross-П РС когнітивної мережі в умовах радіоелектронної протидії</i>	377
6.5.1.	<i>Розробка захищеного абонентського терміналу, використовуваного при експериментальному дослідженні ..</i>	377
6.5.2.	<i>Особливості моделювання процесу обміну інформацією в системі «точка-точка» в умовах радіоелектронної протидії</i>	381

6.5.3. <i>Особливості моделювання в ЗСП алгоритмів адаптивного управління когнітивною мережею в умовах радіоелектронної протидії</i>	384
6.5.4. <i>Результати дослідження залежності узагальненого комплексного показника якості сигналу у захищених радіоканалах когнітивної мережі</i>	386
Висновки до розділу 6	390
РОЗДІЛ 7 РОЗРОБКА АБСТРАКТНОЇ АРХІТЕКТУРИ ІНТЕЛЕКТУАЛЬНОГО ЕКЗОФАКТОРА МОНІТОРИНГУ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА МЕТОДІВ ЇЇ РЕАЛІЗАЦІЇ	394
7.1. Вибір підходу до створення концепції екзофактора моніторингу інцидентів інформаційної безпеки.....	394
7.2. Формулювання поняття про EF MISI	395
7.3. Визначення областей застосування екзофакторно-орієнтованого підходу для моніторингу зон безпеки	397
7.4. Розробка абстрактної архітектури EF MISI	399
7.4.1. <i>Реалізація EF MISI, який засновано на реагуванні</i>	402
7.4.2. <i>Реалізація EF MISI, який засновано на сприйнятті</i>	402
7.4.3. <i>Реалізація EF MISI зі станом</i>	404
7.4.4. <i>Реалізація EF MISI з самонавчанням</i>	406
7.4.5. <i>Реалізація EF MISI, який управляється цілями</i>	407
7.4.6. <i>Реалізація функції планування в екзофакторі моніторингу</i>	411
7.4.7. <i>Реалізація функції намірів та розробка ментальної архітектури EF MISI</i>	413
7.5. Розробка методу проектування та реалізації EF MISI.....	416
7.5.1. <i>Визначення цільових завдань EF MISI</i>	417
7.5.2. <i>Формування функції прогнозування</i>	418
7.5.3. <i>Формування функції планування</i>	419
7.5.4. <i>Розробка багат шарового EF MISI</i>	420
7.6. Рішення модельного завдання керування автономним пошуком безпечних зон у межах контрольованої мережевої структури	423
7.6.1. <i>Розробка EF MISI, який ґрунтується на методах формальної логіки</i>	424

7.6.2. Розробка EF MISI, який ґрунтується на методах повного перерахування	429
<i>Висновки до розділу 7</i>	431
РОЗДІЛ 8 РОЗРОБКА ФОРМАЛЬНОЇ МОДЕЛІ КОГНІТИВНОЇ МЕРЕЖІ, ЯКА ЗАБЕЗПЕЧУЄ ФУНКЦІОНУВАННЯ СПЕЦІАЛІЗОВАНИХ ЕКЗОФАКТОРІВ МОНІТОРИНГУ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ПРОЦЕСИ МІГРАЦІЇ ДАНИХ ДО БЕЗПЕЧНИХ СЕГМЕНТІВ	433
8.1. Передумови розробки формальної моделі когнітивної мережі ...	433
8.2. Розробки формальної моделі когнітивної мережі	441
8.3. Аналіз політик комутації при переміщенні даних до безпечних зон когнітивної мережі	449
8.4. Концепція трирівневої мови специфікацій політик маршрутизації при міграції даних	451
<i>Висновки до розділу 8</i>	454
РОЗДІЛ 9 ВИБІР ЗАСОБІВ ТА МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМАХ ДОКУМЕНТООБИГУ ПІДПРИЄМСТВ	455
<i>Висновки до розділу 9</i>	474
ЗАГАЛЬНІ ВИСНОВКИ	475
Список літературних першоджерел	489

ЛІТЕРАТУРНЕ ПОСИЛАННЯ НА РЕСУРС

Удосконалення принципів та методів інформаційного забезпечення, інформаційної та фінансово-економічної безпеки підприємств та організацій сфери економіки, бізнесу та фінансів [Звіт про НДР] : (проміжн.) / О. О. Скопа, О. В. Орлик, Н. Ф. Казакова, Ю. В. Щербина, С. В. Волков, О. В. Грабовський, В. А. Лахно, О. І. Мацків, О. Г. Єсіна, А. Ю. Вакула, О. О. Фразе-Фразенко, О. О. Йона, Є. В. Вавилов, К. Б. Айвазова, С. Д. Асабашвілі // ОНЕУ ; кер. О. О. Скопа. – 0112U007713. – Одеса, 2014. – 527 с.

ВСТУП

Підстави для проведення науково-дослідної роботи

В епоху глобалізації та постіндустріального етапу розвитку все більшого значення набуває інформація. У цій ситуації однією з найважливіших складових національної і, т.ч., економічної безпеки є інформаційна політика держави.

Інтеграція сучасних інформаційних технологій істотно змінила міжнародні відносини. Одним з ключових напрямків трансформації стає реалізація економічних інтересів шляхом забезпечення інформаційної безпеки. Інформаційна безпека має своє відображення в нормативно-правовій базі України, а саме - в Законах України «Про національну програму інформатизації», «Про концепцію національної програми інформатизації», а також у «Стратегії національної економічної безпеки України», яка затверджена Указом Президента України.

Згідно Законом України «Про концепцію національної програми інформатизації», інформаційна безпека - це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому унеможлиблюється нанесення шкоди шляхом недостовірної, неточної, несвоєчасної інформації, яка використовується; негативний інформаційний вплив, негативні наслідки використання інформаційних технологій, несанкціоноване поширення, порушення цілісності і т.д.

У Законі України «Про основи національної безпеки» вперше дана офіційна оцінка значимості економічної безпеки, як невід'ємної складової економічної безпеки України.

У «Стратегії національної економічної безпеки України» зазначено:

- посилюється негативний зовнішній вплив на інформаційний простір України, що загрожує розмиванням суспільних цінностей і національної ідентичності;

- залишаються недостатніми обсяги вироблення конкурентоспроможного національного інформаційного продукту;

- наближається до критичного стан безпеки інформаційно-комп'ютерних систем в галузі державного управління, фінансової і банківської сфери, енергетики, транспорту, внутрішніх та міжнародних комунікацій тощо.

Необхідність забезпечення інформаційної безпеки зумовлена насамперед тим, що на сьогоднішній день існують загрози інформаційній сфері країни, які можуть завдати значної шкоди національним інтересам. Серед основних інформаційних загроз можна виділити наступні:

- прояви обмеження свободи слова та доступу громадян до інформації;
- поширення засобами масової інформації культу насильства, комп'ютерна злочинність та комп'ютерний тероризм;
- розголошення інформації, що становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;
- спроби маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Інформаційна безпека є складним, системним, багаторівневим явищем, стан і перспективи розвитку якого мають безпосередній вплив на зовнішні і внутрішні чинники, найважливішими з яких є:

- 1) політична обстановка у світі;
- 2) наявність потенційних зовнішніх і внутрішніх загроз;
- 3) стан і рівень інформаційно-комунікаційного розвитку країни;
- 4) внутрішньополітична обстановка в країні.

Важливим для інформаційної безпеки держави є досягнення стану її захищеності, тобто створення і підтримка відповідних інженерно-технічних потужностей та інформаційної організації, що відповідають реальним і потенційним загрозам, а також рівня демографічного та економічного становища країни.

Питання забезпечення інформаційної безпеки актуальні в тій чи іншій мірі для всіх держав. Однак питома вага інженерно-технічних і апаратно-програмних методів забезпечення національної безпеки у різних держав неоднакова і залежить від цілого комплексу умов, пов'язаних з імовірністю внутрішніх і зовнішніх загроз, характером відносин з суміжними державами та геополітичними центрами.

По своїй загальній спрямованості загрози інформаційній безпеці України можна розділити на такі види:

- 1). Загрози конституційним правам і свободам людини і громадянина у сфері духовного життя та інформаційної діяльності, індивідуальній, груповій та суспільній свідомості, духовному відродженню України.
- 2). Загрози інформаційному забезпеченню державної політики України.
- 3). Загрози розвитку вітчизняної індустрії інформації, включаючи індустрію засобів інформатизації, телекомунікацій і зв'язку.
- 4). Загрози безпеці інформаційно-телекомунікаційних систем на території України, як діючих, так і тих, які створюються.

Основні шляхи та напрямки реалізації концептуальних положень інформаційної безпеки держави повинні бути визначені в науково обґрунтованій доктрині інформаційної безпеки, якої на сьогодні в Україні немає. Вона, як правило, розробляються на певний період і є керівництвом до дії. На основі доктринальних положень здійснюється широке коло політичних заходів і дій в зовнішній і внутрішній політиці держави. Доктрина інформаційної безпеки, будучи логічним продовженням «Стратегії національної безпеки», розробляється законодавчими органами і політичним керівництвом держави. Її основні вимоги деталізуються в законодавчому та іншому нормативно-правовому акті, висвітлені в стратегії розвитку держави у вигляді цільових державних програм і проектів.

Для захисту національного інформаційного простору та ресурсів повинні використовуватися адекватні методи і засоби, які базуються на відповід-

них сучасних інформаційних та інформаційно-аналітичних технологіях. Серед них можна назвати наступні:

- правове регулювання і контроль;
- економічне (податкове, тарифне, митне і т.д.) регулювання і контроль;
- державне ліцензування та сертифікація суб'єктів національного інформаційного простору України;
- технічний та програмний захист.

Варто розуміти, що тільки формування комплексної інформаційної політики допоможе підтримати національний суверенітет української держави і сформувати в суспільстві єдину національну позицію.

Аналіз теоретико-методологічних основ явища інформаційної безпеки держави та її економіки в умовах сучасного стану і перспектив розвитку української державності, а також результати історичного розвитку суспільства дають підставу зробити наступні висновки:

1). Інформаційна безпека держави являє собою такий стан інститутів держави і суспільства, при якому забезпечується надійний захист національних інтересів країни та її громадян в інформаційній сфері.

2). Обов'язок забезпечення інформаційної безпеки, як невід'ємної складової національної безпеки, покладається на інформаційну організацію державами

3). Інформаційна організація держави має бути гарантом інформаційної безпеки держави та її інститутів, суспільства і громадян, стабільності політичного режиму в умовах процесів глобалізації.

4). Актуальним науковим і практичним завданням у сфері забезпечення інформаційної безпеки України є досягнення єдиного підходу до визначення оптимальних моделей і шляхів забезпечення інформаційної безпеки держави на основі виявлення найважливіших якісних і кількісних параметрів цього явища.

Проблеми інформаційної безпеки, удосконалення принципів та методів інформаційного забезпечення, інформаційної та фінансово-економічної без-

пеки підприємств та організацій сфери економіки, бізнесу та фінансів України в сучасних умовах надзвичайно актуальні та потребують поглибленого вивчення.

Термін «безпека» розуміється як стан захищеності життєво важливих інтересів особистості, підприємства, суспільства, держави від внутрішніх і зовнішніх загроз. Але його зміст у науковому розумінні ще повністю не визначено. Сьогодні йде дискусія навколо цього питання, зокрема - навколо оцінки критеріїв безпеки, характеристик можливих небезпек та їх структури або принципів побудови системи забезпечення безпеки підприємств та організацій.

Одночасно менеджери підприємств та організацій сфери економіки, бізнесу та фінансів відчувають певний дефіцит спеціальної літератури з питань правового освітлення сучасних проблем інформаційного права. Незважаючи на вихід у світ багатьох видань і наукових статей, висвітлені ці проблеми лише в загальному. Крім того, в сучасній науковій та навчальній літературі дуже часто не завжди адекватно висвітлено проблеми методології забезпечення інформаційних процесів або недостатньо фактичного матеріалу.

При аналізі проблем інформаційної безпеки в методологічному плані найбільш важливим є:

- визначення та обґрунтування понятійного апарату;
- налагодження структурно-функціональних зв'язків базових понять і розробка на цій основі відповідних нормативно-правових основ системи інформаційної безпеки;
- удосконалення системи управління інформаційною безпекою на державному та місцевому рівнях у галузі інформаційного забезпечення, інформаційної та фінансово-економічної безпеки підприємств та організацій сфери економіки, бізнесу та фінансів;
- визначення критеріїв ефективності функціонування системи інформаційної безпеки в різних сферах життя і діяльності суспільства (політичної, економічної, науки і техніки, духовної і т.д.).

У цілому система інформаційної безпеки повинна відображати стан захищеності як національних інтересів саме в інформаційній сфері від зовнішніх і внутрішніх загроз як для самої держави або суспільства, так і окремих підприємств та організацій сфери економіки, бізнесу та фінансів.

Система інформаційної безпеки є одночасно і елементом у системі вищого рівня - міжнародного, національного, місцевого. Але сьогодні ряд підсистем, що входять в цю макросистему, ще не вивчені на належному рівні, а також не мають комплексного, системного дослідження з виходом на сучасні конструкції та пропозиції. Це стосується проблем інформаційної безпеки підприємств та організацій сфери економіки, бізнесу та фінансів в Україні.

Вивчення науково-теоретичних і практичних проблем інформаційної безпеки у зазначеній галузі дозволить визначити і вирішити завдання щодо створення систем інформаційної безпеки, які б функціонували ефективно.

Головним завдання інформаційної безпеки підприємств та організацій сфери економіки, бізнесу та фінансів, є визначення національних інтересів в інформаційній сфері, виявлення загроз, їх класифікація, пошук та надання оптимальних засобів, що дозволяють забезпечити створення стійкої системи інформаційної безпеки у досліджуваній галузі.

Мета НДР

Зважаючи на вище приведене, метою НДР є виконання теоретичних досліджень щодо удосконалення існуючих принципів та методів інформаційного забезпечення, інформаційної та фінансово-економічної безпеки підприємств та організацій сфери економіки, бізнесу та фінансів

Основні завдання для досягнення мети

Основними завданням для досягнення мети роботи є розробка та удосконалення методологій, методик, методів та засобів щодо збереження та за-

хисту інтелектуальної власності, конфіденційної клієнтської інформації та іншої інформації, що має критично важливе значення для ведення бізнесу у вигляді стратегій або окремих рішень у сфері безпеки, які тісно ув'язані з цілями та завданнями бізнесу, у тому числі:

- *управління ідентифікаційною інформацією і доступом;*
- *управління інформаційною та фінансово-економічною безпекою підприємств;*
- *конфіденційність та захист даних;*
- *забезпечення виконання стандартів та нормативних вимог підприємствами та організаціями;*
- *управління загрозами та уразливостями;*
- *забезпечення фізичної безпеки;*
- *тестування на проникнення у системи захисту від несанкціонованого доступу;*
- *удосконалення архітектури інформаційної безпеки;*
- *забезпечення дотримання законодавчих вимог та політик підприємств та організацій сфери економіки, бізнесу та фінансів;*
- *питання інформаційної безпеки у галузі поінформованості та навчання співробітників;*
- *питання підготовки кадрів та підвищення кваліфікації співробітників підприємств та організацій сфери економіки, бізнесу та фінансів у галузі інформаційної та фінансово-економічної безпеки.*

Взаємозв'язок з іншими роботами

НДР за темою «Удосконалення принципів та методів інформаційного забезпечення, інформаційної та фінансово-економічної безпеки підприємств та організацій сфери економіки, бізнесу та фінансів» виконується вперше та не базується на НДР ОНЕУ, які виконувалися раніше.

З ПОВНИМ ТЕКСТОМ ЗВІТУ МОЖНА ОЗНАЙОМИТИСЯ У БІБЛІОТЕЦІ НАУКОВО-ДОСЛІДНОГО ВІДДІЛУ ОДЕСЬКОГО НАЦІОНАЛЬНОГО ЕКОНОМІЧНОГО УНІВЕРСИТЕТУ

АННОТАЦІЯ

У звіті висвітлено наступні наукові та практичні здобутки:

Встановлено, що всі види безпеки тісним чином взаємозв'язані та переплетені. Відповідно, забезпечення економічної безпеки у сфері економіки та бізнесу з точки зору її організації недержавними структурами, не зважаючи на зазначені делеговані їм функції, недоцільно обмежувати захистом особи та офісу, матеріальних та фінансових ресурсів від дії деструктивних соціальних сил без врахування технічних, природних та інших чинників, які, начебто, не відносяться до областей їх діяльності. Швидке зростання видів та напрямів загроз економічній безпеці викликає адекватну реакцію щодо створення систем захисту.

Показано, що вибір підприємством конкретних засобів і шляхів забезпечення його економічної безпеки обумовлюється характером і масштабом загроз економічним інтересам підприємства. Всі компоненти системи економічної безпеки пов'язані між собою, і тільки їх комплексне застосування забезпечує успіх функціонування й розвитку підприємства як цілісної системи.

Встановлено, що світова і вітчизняна практика безпеки свідчать: щоб ефективно протидіяти загрозам і створювати умови безпечної і стабільної роботи підприємства, необхідно не тільки створити систему комплексного захисту, але і забезпечити її раціональне функціонування. Існує велика кількість чинників, що породжують загрози економічній безпеці підприємства. Рівень економічної безпеки базується на тому, наскільки ефективно

службам підприємства вдається забезпечувати контроль за ситуацією, запобігати загрозам й усувати збитки від негативних впливів на різні аспекти економічної безпеки.

Показано, що забезпечення надійної системи економічної безпеки підприємства – постійний процес, спрямований на своєчасне виявлення, попередження і нейтралізацію різних видів загроз економічній безпеці підприємства з метою запобігання можливим збиткам, а також забезпечення стійкого і максимально ефективного функціонування підприємства тепер і в майбутньому.

Визначено, що в сучасних умовах для підприємств України пріоритетне значення має проблема забезпечення їх фінансово-економічної безпеки шляхом запровадження відповідного механізму управління і ефективного використання його складових. Механізм забезпечення фінансово-економічної безпеки є невід’ємним елементом системи безпеки підприємства і передбачає використання сукупності методів, інструментів та заходів їх реалізації, які необхідно використовувати не розрізнено, а у поєднанні.

Показано, що в умовах постійного ризику та протидії зловмисникам, система економічної безпеки суб’єкта господарювання повинна: бути дієвою, постійно захищаючи його інтереси; виявляти різноманітні деструктивні фактори, вживати заходи щодо попередження їх шкідливого впливу та нанесення збитків суб’єкту господарювання.

Показано, що забезпечення надійної й ефективною системи економічної безпеки – постійний процес, спрямований на своєчасне виявлення, попередження і нейтралізацію різних видів загроз економічній безпеці з метою запобігання можливим збиткам, а також забезпечення стійкого і максимально ефективного функціонування суб’єкта господарювання.

Встановлено, що проблема охорони авторських прав на бази даних урегульована на недостатньому рівні, що ускладнює організацію захисту баз даних у межах закону.

Показано, що завдання вивчення та створення інтелектуальних автономних систем для галузі економіки, бізнесу та фінансів, цілком може пре-

тендувати на статус цілеорієнтовної задачі, яка може бути викликом сучасним та перспективним інформаційним технологіям. Завдання задоволення тим вимогам, які були сформульовані у введенні до проблеми.

Визначено особливості формули для розрахунку статистики при обмеженому числі об'єктів системи, яка підлягає випробуванням.

Отримано нові властивості неповної β -функції.

Приведено нове трактування процесу прогнозування, яке не суперечить тим положенням, які викладені у літературі. Показано, що його можна вважати достатньо адекватними та такими, що є універсальним як при використанні у звичайних системах прогнозування, так і у таких, що базуються на генетичних алгоритмах.

Розглянуто етапи прогнозування, які можуть бути реалізовані засобами нейронних мереж із застосуванням аналітичних методів, експертних систем, методів математичної статистики, нечіткої логіки та статистики об'єктів нечислової природи, дають можливість незалежно від сфери застосування систем прогнозування, отримати необхідні дані щодо стану досліджуваної соціальної, економічної або технічної системи.

Встановлено, що з метою впровадження у навчальний процес матеріалів стосовно захисту інформації у галузі економіки, бізнесу та фінансів, є доцільним проведення досліджень у обсягах, які б забезпечили рішення проблеми. При цьому показано, що є доцільним провести історичний огляд проблеми захисту інформації; дати поняття про задачі, що вирішуються криптографічними методами; розглянути формалізацію процесів у криптографічних системах; навести відомості про надмірність текстів, їх математичну модель та математичні критерії на відкритий текст; розглянути умови побудови досконалих шифрів; привести параметри сучасних шифрів; дати поняття про елементарні криптографічні перетворення, включаючи поняття про підстановку, як основне криптографічне перетворення; привести відомості про математичні моделі шифрів заміни та про загальні підходи до будовання композиційних шифрів; привести

огляд сучасних симетричних криптографічних систем та загальних особливостей побудови блочних симетричних криптографічних систем.

Представлено матеріали, які описують організацію інформаційної взаємодії між клієнтами мережі Інтернет на мережевому рівні моделі OSI. Розглянуто один з найбільш важливих компонентів взаємодії - структура блоку даних каналного рівня.

Показано, що Internet, це зв'язна сукупність кінцевих або проміжних вузлів, що мають однакову адресу мережі. Відзначено, що кожен з вузлів даної мережі має унікальну мережеву адресу. Для забезпечення інформаційної взаємодії у середині мережі може бути використано кожний з протоколів каналного рівня. Показано, що максимальне число вузлів у мережі визначається типом використовуваного протоколу мережевого рівня. Мережа мінімального розміру може включати тільки один вузол.

Відзначено, що для забезпечення інформаційної взаємодії між мережами використовуються спеціальні мережеві компоненти, тобто маршрутизатори. Вони є спеціалізованими обчислювальними ЕОМ, завданням яких є визначення ділянки маршруту, по якій повинен бути переданий кожен з пакетів, що до нього входять. Описані процедури передавання.

Відзначено, що таблиця маршрутизації може бути побудована різними способами, які докладно розглянуті в розділі. Відзначено, що для успішного функціонування маршрутизатора його таблиця маршрутизації не обов'язково повинна містити стільки записів, скільки мереж є в Internet.

Розглянуто умову забезпечення енергетичної скритності передавання сигналів елементами Cross-П РС, які відносяться до когнітивної мережі, на основі сигнальних конструкцій реалізацій динамічного хаосу.

Показано можливість використання багаторівневих послідовностей як розширювальних послідовностей інформаційного сигналу для підвищення скритності передачі.

Отримано результат про те, що існує характерний протилежний взаємозв'язок між показниками енергетичної скритності та завадостійкості.

Це підтверджено даними імітаційного моделювання та показано, що поліпшення одного показника приводить до погіршення іншого.

Показано, що з розвитком когнітивних мереж у них передбачається висока щільність цифрових радіозасобів, що створюватиме великий рівень взаємних завад внаслідок істотного розширення смуги займаних частот та загострення проблеми несумісності сигналів стандарту IEEE 802.16 з існуючим парком апаратури. Відзначено відсутність єдиного стандарту на пропонуване рішення стосовно створення EF MISI у межах когнітивної мережі

Запропоновано метод сумісного передавання аналогових сигналів у існуючих системах, які можуть бути задіяні у складі інтегрованого платформного середовища, та цифрових даних від систем управління СЗІ та інших систем реагування на інциденти інформаційної безпеки, з одночасним забезпеченням суттєвого зниження рівня шумів у комунікаційному тракті.

Відзначено, що впровадження методу формування спектру сигналу для Cross-П РС когнітивної мережі, дозволяє зберегти структуру частот радіодіапазону, яка існує на поточний час, та, як побічний позитивний ефект, забезпечує більш якісні показники при організації стереофонічного радіомовлення.

Доведено, що при впровадженні методу формування спектру сигналу для Cross-П РС когнітивної мережі, завадозахищенність структур управління системами захисту інформації значно зростає внаслідок того, що канали Cross-П РС стають нечутливими до засобів радіоелектронної протидії.

Запропоновано структуру передавального тракту, який дозволяє використати не задіяні смуги частот у спектрах, де ведеться радіомовлення та на які можуть впливати системи РЕП, для передавання низькошвидкісного групового потоку або широкосмугового сигналу від структур управління системами захисту інформації, від систем монітору інформаційного простору когнітивної мережі та даних про інциденти інформаційної безпеки та ін., а з

використанням відповідних несійних коливань, без порушення існуючої структури спектрів, передавати ті ж сигнали у діапазонах, передбачених, наприклад, стандартом IEEE 802.16, та використовувати для міграції даних у безпечні зони.

Показано, що в умовах радіоелектронної протидії функціонуванню Cross-П РС когнітивної мережі найбільшу небезпеку представляють адитивні навмисні перешкоди, зокрема, фазовані імітаційні завади з обмеженою середньою потужністю та особливою структурою кадру накладання. Відзначено, що при їх використанні ефективність стандартних алгоритмів шифрування та завадостійкого кодування різко знижується через порушення синхронізації. Досягнуто рішення зазначеної проблеми шляхом створення та застосування цифрового прецизійного часового дискримінатора нової структури на який отримано патент України.

Розроблено експериментальну схему організації зв'язку за принципом «точка-точка» через СМСЗ стандарту CDMA, яка включає синтезовані оригінальні захищені пристрої, базові станції, інтегровані пристрої шифрування, радіотелефони стандарту CDMA, дослідний центр комутації мобільного зв'язку, програмно-апаратний генератор завад, програмно-апаратні пристрої контролю та управління, цифровий прецизійний числовий дискримінатор та програмно-апаратний генератор хаотичних сигналів.

Показано, що використання засобів підвищення завадостійкості, які реалізовані методом управління загальною синхронізацією на основі запропонованого цифрового частотного дискримінатора, позитивно впливають на залежність своєчасної доставки сигналів $P_{\text{своєчас}}$ від комплексного показника якості \vec{K} .

Встановлено, що створення інтелектуальних екзофакторів моніторингу та мультиекзофакторних систем контролю за подіями інформаційної безпеки та іншими деструктивними впливами, є однією з найбільш перспективних областей як теоретичних, так і практичних досліджень стосовно систем захисту інформації.

ЗАГАЛЬНІ ВИСНОВКИ

Матеріали, представлені у звіті, дозволяють зробити висновки про наступне:

1) Всі види безпеки тісним чином взаємозв'язані та переплетені. Відповідно, забезпечення економічної безпеки у сфері економіки та бізнесу з точки зору її організації недержавними структурами, не зважаючи на зазначені делеговані їм функції, недоцільно обмежувати захистом особи та офісу, матеріальних та фінансових ресурсів від дії деструктивних соціальних сил без врахування технічних, природних та інших чинників, які, начебто, не відносяться до областей їх діяльності. Швидке зростання видів та напрямів загроз економічній безпеці викликає адекватну реакцію щодо створення систем захисту. Для сучасних вітчизняних суб'єктів господарювання абстрактні поняття про безпеку бізнесу поступово трансформуються в реальні події. Їх передбачення та усунення практично неможливе без залучення недержавних структур з організації безпеки. Ефективне рішення питання безпечної підприємницької діяльності потребує створення комплексної системи управління безпекою на підприємстві, де б поєднувалися зусилля держави, спеціальних органів, окремих підприємств та недержавних структур забезпечення безпеки бізнесу. Одним з ключових завдань в побудові комплексної системи забезпечення безпеки українських підприємств є підготовка висококваліфікованих фахівців в даній галузі.

2) Вибір підприємством конкретних засобів і шляхів забезпечення його економічної безпеки обумовлюється характером і масштабом загроз економічним інтересам підприємства. Всі компоненти системи економічної безпеки пов'язані між собою, і тільки їх комплексне застосування забезпечує успіх функціонування й розвитку підприємства як цілісної системи.

3) Світова і вітчизняна практика безпеки свідчать: щоб ефективно протидіяти загрозам і створювати умови безпечної і стабільної роботи підприємства, необхідно не тільки створити систему комплексного захисту,

але і забезпечити її раціональне функціонування. Існує велика кількість чинників, що породжують загрози економічній безпеці підприємства. Рівень економічної безпеки базується на тому, наскільки ефективно службам підприємства вдається забезпечувати контроль за ситуацією, запобігати загрозам й усувати збитки від негативних впливів на різні аспекти економічної безпеки.

4) Забезпечення надійної системи економічної безпеки підприємства – постійний процес, спрямований на своєчасне виявлення, попередження і нейтралізацію різних видів загроз економічній безпеці підприємства з метою запобігання можливим збиткам, а також забезпечення стійкого і максимально ефективного функціонування підприємства тепер і в майбутньому.

5) В сучасних умовах для підприємств України пріоритетне значення має проблема забезпечення їх фінансово-економічної безпеки шляхом запровадження відповідного механізму управління і ефективного використання його складових. Механізм забезпечення фінансово-економічної безпеки є невід’ємним елементом системи безпеки підприємства і передбачає використання сукупності методів, інструментів та заходів їх реалізації, які необхідно використовувати не розрізнено, а у поєднанні.

6) В умовах постійного ризику та протидії зловмисникам, система економічної безпеки суб’єкта господарювання повинна: бути дієвою, постійно захищаючи його інтереси; виявляти різноманітні деструктивні фактори, вживати заходи щодо попередження їх шкідливого впливу та нанесення збитків суб’єкту господарювання. Це дасть можливість зменшити витрати, оскільки економічно вигідніше є вчасне виявлення можливих загроз і небезпек, та проведення відповідних заходів їх попередження, ніж усунення завданої ними шкоди. Система економічної безпеки повинна бути такою, щоб витрати на її забезпечення були економічно обґрунтованими, оптимальними і доцільними, і не перевищували той граничний рівень, при якому втрачається економічна доцільність їх застосування.

7) Забезпечення надійної й ефективної системи економічної безпеки – постійний процес, спрямований на своєчасне виявлення, попередження і нейтралізацію різних видів загроз економічній безпеці з метою запобігання можливим збиткам, а також забезпечення стійкого і максимально ефективного функціонування суб'єкта господарювання.

8) Проблема охорони авторських прав на бази даних урегульована на недостатньому рівні, що ускладнює організацію захисту баз даних у межах закону. Основними проблемами, які потребують додаткового дослідження та вирішення, є:

1 встановлення уніфікованої термінології, що стосується інформаційної сфери;

2 забезпечення охорони комп'ютерних програм та баз даних, а саме визначення:

– основних засад правової охорони використання комп'ютерних програм та баз даних;

– переліку випадків, що кваліфікуються як неправомірне використання комп'ютерних програм та баз даних;

– санкцій за неправомірне використання комп'ютерних програм та баз даних.

9) Завдання вивчення та створення інтелектуальних автономних систем для галузі економіки, бізнесу та фінансів, цілком може претендувати на статус цілеорієнтовної задачі, яка може бути викликом сучасним та перспективним інформаційним технологіям. Завдання задовольняє тим вимогам, які були сформульовані у введенні до проблеми. Воно допускає широкий діапазон постановок, які можуть змінюватися як по рівню спільності (від концептуальних до конкретно-алгоритмічних), так і по складності вирішуваних задач. Т.ч. завдання забезпечує необхідну масштабованість підходу. У свою чергу, таке варіювання приводить до необхідності залучення в процес вивчення та створення ІАС всіх без виключення дисциплін, пов'язаних з ІІС.

10) Визначено особливості формули для розрахунку статистики при обмеженому числі об'єктів системи, яка підлягає випробуванням, а саме:

- у випадку контрольних випробувань об'єктів системи по біноміальній схемі з зупинками отриманий результат поки є єдиним і найкращим у використовуваній схемі випробувань;
- отримана статистика може бути використана тоді, коли контрольні випробування кожного з об'єктів проводяться по біноміальній схемі Бернуллі;
- при безвідмовних випробуваннях всіх об'єктів з виразу для статистики впливає часткове значення, яке для випадку контрольних випробувань об'єктів по біноміальній схемі Бернуллі, може бути розцінено як несподіваний і парадоксальний результат. Однак, проведений аналіз граничної ситуації усуває видиму парадоксальність;
- отримані формул розрахунку надійності мають простий аналітичний вигляд, що є великою рідкістю в задачах такого типу, які часто приводять до необхідності складних обчислень на ЕОМ.

11) Отримано нові властивості неповної β -функції, які приведено у таблиці.

12) Показано, що отримана у 4 розділі багатокритеріальна модель забезпечує вибір точки розв'язку на множині Парето. При цьому зазначено, що слід враховувати задані обмеження на допустиму область зміни векторного критерію, якщо множина Парето належить цій області. Відповідно, для розв'язання багатокритеріальних задач, у яких задані обмеження на компонентах векторного критерію, рекомендується використовувати запропоновану модель. При цьому слід враховувати недоліки зазначеної моделі:

- громіздкість рівнянь при великій розмірності;
- СНР може мати багато коренів;
- якщо розв'язок лежить на границях обмежень, то він буде знайде-

ний з похибкою, хоча й меншою, ніж необхідна (тобто це значить, що немає принципово точного розв'язку).

13) Приведено нове трактування процесу прогнозування, яке не суперечить тим положенням, які викладені у літературі. Показано, що його можна вважати достатньо адекватними та такими, що є універсальним як при використанні у звичайних системах прогнозування, так і у таких, що базуються на генетичних алгоритмах. По своїй ролі в управлінні, по своєрідності змісту та по спільності форм і методів реалізації зазначених етапів у прогнозуванні, суть їх залишається зрозумілою та забезпечує виконання найважливіших його функцій. Прогнозування на їх основі залишається максимально значимим і може розгортатися достатньо інтенсивно при визначенні точних його цілей.

14) Розглянуто етапи прогнозування, які можуть бути реалізовані засобами нейронних мереж із застосуванням аналітичних методів, експертних систем, методів математичної статистики, нечіткої логіки та статистики об'єктів нечислової природи, дають можливість незалежно від сфери застосування систем прогнозування, отримати необхідні дані щодо стану досліджуваної соціальної, економічної або технічної системи. Т.ч., до ситуаційної методології прогнозування можна внести пункт про те, що вона може містити приведені етапи, які не суперечить загально прийнятим уявленням.

15) Встановлено, що з метою впровадження у навчальний процес матеріалів стосовно захисту інформації у галузі економіки, бізнесу та фінансів, є доцільним проведення досліджень у обсягах, які б забезпечили рішення проблеми. При цьому показано, що є доцільним провести історичний огляд проблеми захисту інформації; дати поняття про задачі, що вирішуються криптографічними методами; розглянути формалізацію процесів у криптографічних системах; навести відомості про надмірність текстів, їх математичну модель та математичні критерії на відкритий текст; розглянути умови побудови досконалих шифрів; привести параметри сучасних шифрів; дати поняття про елементарні криптографічні перетво-

рення, включаючи поняття про підстановку, як основне криптографічне перетворення; привести відомості про математичні моделі шифрів заміни та про загальні підходи до будування композиційних шифрів; привести огляд сучасних симетричних криптографічних систем та загальних особливостей побудови блочних симетричних криптографічних систем.

Отримані рішення дозволяють удосконалити навчальні матеріали з дисциплін, які викладаються кафедрою при підготовці фахівців галузі економіки, бізнесу та фінансів.

16) Представлені у звіті матеріали описують організацію інформаційної взаємодії між клієнтами мережі Інтернет на мережевому рівні моделі OSI. Розглянуто один з найбільш важливих компонентів взаємодії - структура блоку даних каналного рівня. Відзначено, що блок призначений для доставки щодо невеликого фрагмента переданого повідомлення. Показано, що для забезпечення можливості доставки цього фрагмента кожен пакет забезпечується мережевою адресою пункту призначення й адресою джерела даного повідомлення. Описані всі процедури й поля, зв'язані адресацією даних, захистом, обробкою і т.д. На підставі наведених даних показано, що кожний з пакетів має можливість переміщатися по мережі незалежно від інших пакетів, які використовуються для доставки інших компонентів цього ж повідомлення. Прикладами аналогічних протоколів мережного рівня є такі протоколи, як X.25, IPX, Apple Talk, однак у цей час найбільше поширення має Internet протокол - IP.

17) Показано, що Internet, це зв'язна сукупність кінцевих або проміжних вузлів, що мають однакову адресу мережі. Відзначено, що кожен з вузлів даної мережі має унікальну мережеву адресу. Для забезпечення інформаційної взаємодії у середині мережі може бути використано кожний з протоколів каналного рівня. Показано, що максимальне число вузлів у мережі визначається типом використовуваного протоколу мережевого рівня. Мережа мінімального розміру може включати тільки один вузол.

18) Відзначено, що для забезпечення інформаційної взаємодії між мережами використовуються спеціальні мережеві компоненти, тобто маршрутизатори. Вони є спеціалізованими обчислювальними ЕОМ, завданням яких є визначення ділянки маршруту, по якій повинен бути переданий кожен з пакетів, що до нього входять. Описані процедури передавання. Показано, що завдання визначення шляхів, які повинні привести даний пакет у пункт його призначення, маршрутизатор вирішує локальним образом - він визначає тільки номер свого інтерфейсу, через який цей пакет повинен бути відправлений.

19) Відзначено, що таблиця маршрутизації може бути побудована різними способами, які докладно розглянуті в розділі. Відзначено, що для успішного функціонування маршрутизатора його таблиця маршрутизації не обов'язково повинна містити стільки записів, скільки мереж є в Internet. Показано, що в тому випадку, якщо не вдається визначити напрямок передавання пакета звичайним способом, маршрутизатор передає його в напрямку шлюзу, який визначений у якості default gateway для даного маршрутизатора.

20) З метою удосконалення технологій забезпечення захисту інформації у когнітивних структурах, а саме - у елементами Cross-П РС, в умовах електронної протидії:

- *розглянуто умову забезпечення енергетичної скритності передавання сигналів елементами Cross-П РС, які відносяться до когнітивної мережі, на основі сигнальних конструкцій реалізацій динамічного хаосу;*
- *показано можливість використання багаторівневих послідовностей як розширювальних послідовностей інформаційного сигналу для підвищення скритності передачі, та проведено імітаційне моделювання когнітивної мережі з елементами Cross-П РС, у яких є доцільним використання хаотичних сигналів;*

- з врахуванням п. 1 та п. 2 показано, що для підвищення ефективності технологій забезпечення захисту інформації у Cross-П РС в умовах електронної протидії є доцільним використання методів передавання інформації, заснованих на хаотичних сигналах, що забезпечує високі показники як енергетичної скритності, так і структурної;
- з врахуванням п. 3 отримано результат про те, що існує характерний протилежний взаємозв'язок між показниками енергетичної скритності та завадостійкості. Це підтверджено даними імітаційного моделювання та показано, що поліпшення одного показника приводить до погіршення іншого. Акцентовано увагу на тому, що при виборі параметрів передачі елементів Cross-П РС, необхідно знайти компроміс між умовою забезпечення якості передавання та скритності. Можливим варіантом підвищення скритності передачі при збереженні необхідної завадостійкості може бути використання в системі завадостійкого кодування;
- показано, що з розвитком когнітивних мереж у них передбачається висока щільність цифрових радіозасобів, що створюватиме великий рівень взаємних завад внаслідок істотного розширення смуги займаних частот та загострення проблеми несумісності сигналів стандарту IEEE 802.16 з існуючим парком апаратури. Відзначено відсутність єдиного стандарту на пропонуване рішення стосовно створення EF MISI у межах когнітивної мережі. Зроблено висновок про те, що не зважаючи на переваги цифрового способу організації передавання даних у Cross-П РС, існує нагальна потреба використання існуючих аналогових систем для потреб когнітивної мережі;
- для вирішення проблеми, описаної у попередньому пункті, запропоновано компромісний варіант: проміжною ланкою між існуючим та перспективним парком апаратури передавання даних у Cross-П

РС, можуть бути пристрої передавання та приймання, що використовують аналоговий радіосигнал, з застосуванням до нього цифрових методів формування та обробки;

- *запропоновано метод сумісного передавання аналогових сигналів у існуючих системах, які можуть бути задіяні у складі інтегрованого платформного середовища, та цифрових даних від систем управління СЗІ та інших систем реагування на інциденти інформаційної безпеки, з одночасним забезпеченням суттєвого зниження рівня шумів у комунікаційному тракті, що дозволить використати типовий приймач без заміни смугового фільтра різницевого сигналу на фільтр з меншою смугою пропускання, що може привести до зниження капітальних затрат на початковому етапі впровадження Cross-П РС у когнітивній мережі;*
- *відзначено, що впровадження методу формування спектру сигналу для Cross-П РС когнітивної мережі, дозволяє зберегти структуру частот радіодіапазону, яка існує на поточний час, та, як побічний позитивний ефект, забезпечує більші якісні показники при організації стереофонічного радіомовлення;*
- *доведено, що при впровадженні методу формування спектру сигналу для Cross-П РС когнітивної мережі, завадозахищенність структур управління системами захисту інформації значно зростає внаслідок того, що канали Cross-П РС стають нечутливими до засобів радіоелектронної протидії.*

21) Запропоновано структуру передавального тракту, який дозволяє використати не задіяні смуги частот у спектрах, де ведеться радіомовлення та на які можуть впливати системи РЕП, для передавання низькошвидкісного групового потоку або широкосмугового сигналу від структур управління системами захисту інформації, від систем монітору інформаційного простору когнітивної мережі та даних про інциденти інформаційної безпеки та ін., а з використанням відповідних несійних коливань, без порушення іс-

нуючої структури спектрів, передавати ті ж сигнали у діапазонах, передбачених, наприклад, стандартом IEEE 802.16, та використовувати для міграції даних у безпечні зони. Для прийому групового потоку є доцільним використання приймального тракту, опис якого приведено у [410].

22) Показано, що в умовах радіоелектронної протидії функціонуванню Cross-П РС когнітивної мережі найбільшу небезпеку представляють адитивні навмисні перешкоди, зокрема, фазовані імітаційні завади з обмеженою середньою потужністю та особливою структурою кадру накладання. Відзначено, що при їх використанні ефективність стандартних алгоритмів шифрування та завадостійкого кодування різко знижується через порушення синхронізації. Досягнуто рішення зазначеної проблеми шляхом створення та застосування цифрового прецизійного часового дискримінатора нової структури на який отримано патент України.

23) Доведено, що використання цифрового прецизійного часового дискримінатора у структурі інтегрованого платформного середовища когнітивної мережі для потреб СЗІ Cross-П РС, дозволяє значно підвищити точність виміру часових неузгодженостей у системах синхронізації, що веде до більш ефективного задоволення вимог тріади СІА.

24) Розроблено експериментальну схему організації зв'язку за принципом «точка-точка» через СМСЗ стандарту CDMA, яка включає синтезовані оригінальні захищені пристрої, базові станції, інтегровані пристрої шифрування, радіотелефони стандарту CDMA, дослідний центр комутації мобільного зв'язку, програмно-апаратний генератор завад, програмно-апаратні пристрої контролю та управління, цифровий прецизійний числовий дискримінатор та програмно-апаратний генератор хаотичних сигналів, що дозволило виконати експериментальні дослідження щодо визначення залежності узагальненого комплексного показника якості сигналу \vec{K} управління системами захисту інформації від середньої величини $p_{ном}$ при ввімкнених та відімкнених алгоритмі підвищення завадостійкості та системі шифрування в каналах GSM та CDMA, а також вплив на систему шифру-

вання засобів підвищення завадостійкості, які реалізовані методом управління загальною синхронізацією.

25) Показано, що використання засобів підвищення завадостійкості, які реалізовані методом управління загальною синхронізацією на основі запропонованого цифрового частотного дискримінатора, позитивно впливають на залежність своєчасної доставки сигналів $P_{\text{своєчас}}$ від комплексного показника якості \vec{K} , що виражається характерною залежністю у вигляді графіка (рис. 6.12).

26) Обрано 3 вагові коефіцієнти комплексного векторного показника якості сигналу та на основі їх комбінацій, в умовах нормальної сигнально-завадової обстановки, визначено 3 межі ймовірності помилки від дії систем РЕП для сигналу управління системами захисту інформації, тобто межу, коли якість сигналу істотно погіршується (визначено методом експертних оцінок), межу короточасних провалів (визначено включенням системи синхронізації), та межу, коли відбувається порушення синхронізації (крах системи) - $p_{\text{ном}} = (5\dots 8) \cdot 10^{-2}$. Показано, що застосування цифрового частотного дискримінатора дозволяє встановити межу краху інформаційної системи, включаючи СЗІ, за рахунок відновлення синхронізації на рівні ймовірності помилок, де $p_{\text{ном}} \in [(1\dots 8) \cdot 10^{-5}]$.

27) Зазначено, що навмисні перешкоди від систем РЕП можуть спостерігатися на фоні випадкових завад різного характеру, що веде до різкого погіршення якості та провалля сигналу непередбачуваного характеру. Для усунення недоліку запропоновано мотивовану відмова від збалансованості показників $\{\vec{P}; \vec{H}; \vec{I}\}$ у випадку перевищення $p_{\text{ном}}$ встановленого порогу при якому якість сигналу помітно знижується.

28) Встановлено, що створення інтелектуальних екзофакторів моніторингу та мультиекзофакторних систем контролю за подіями інформаційної безпеки та іншими деструктивними впливами, є однією з найбільш перспективних областей як теоретичних, так і практичних досліджень стосовно

систем захисту інформації. З цією метою виконана розробка абстрактної архітектури інтелектуального EF MISI інформаційної безпеки та методів її реалізації. При цьому підставою для досліджень є те, що завдання розробки інтелектуальних екзофакторів моніторингу та мультиекзофакторних систем контролю викликана специфікою сучасних когнітивних інформаційних середовищ спеціального призначення. Її рішення забезпечує когнітивному середовищу достатні можливості для підтримки міграції обчислювальних ресурсів та даних у найбільш безпечні зони. Щодо рішення цього питання, отримано наступні розв'язки, які можуть бути реалізовані у вигляді EF MISI:

- *показано, що EF MISI у змозі вирішити завдання вибору та оцінювання найбільш безпечної зони в межах когнітивного простору, який контролюється, враховуючи його динамічні властивості;*
- *EF MISI дає змогу формування множин даних для розв'язання задач визначення можливості міжрівневої та внутрішньосистемної мобільності інформаційних потоків, включаючи попередні розрахунки пропускну здатності SDN-каналів, які можуть бути використані при міграції обчислювальних ресурсів та даних;*
- *EF MISI дає можливість вирішити завдання вибору оптимальних параметрів використовуваної комунікаційної структури, яка забезпечує міграцію обчислювальних ресурсів та даних;*
- *EF MISI дає змогу вирішити завдання попереднього створення множини регуляризованих операторів для розв'язку некоректних задач, пов'язаних з інцидентами інформаційної безпеки та проблемами відновлення перекручених даних у контрольованому інформаційному просторі;*
- *EF MISI дає змогу вирішити завдання власної адаптації до інцидентів інформаційної безпеки та завдання адаптації до них мережі міграції обчислювальних ресурсів та даних;*
- *EF MISI дає змогу вирішити завдання загального оцінювання на-*

дійності мережі міграції обчислювальних ресурсів та даних.

29) Запропоновані нові методи побудови та впровадження окремого інтелектуального EF MISI, можуть бути основою для інтеграції множини специфічних екзофакторів безпеки в єдину систему. Зважаючи на необхідність рішення наукових задач синтезу методик реалізації та оцінки наскрізної функціональності EF MISI у когнітивних мережах, враховуючи віртуальний характер процесів у пропонованій інтегрованій структурі, яка може бути побудована на базі технологій SDN, у поточному розділі обґрунтовано та виконано наукові дослідження з отриманням нових наукових, технічних та практичних результатів, які можуть бути використані при побудові засобів інформаційної безпеки:

- *запропоновано комбіновану реляційно-автоматну формальну модель, яка охоплює аспекти поведінки когнітивної мережі, які відносяться до міграції даних, що надає можливостей створення імітаційної моделі мережі з метою перевірки дій EF MISI при визначенні ним безпечних зон;*
- *запропоновано варіант формальної мови специфікацій політик комутації пакетів, у якому для опису властивостей досяжності використовується оператор транзитивного замикання відносин комутації пакетів, а для опису властивостей поведінки когнітивної мережі у цілому використовуються темпоральні оператори, що дозволяє вирішувати завдання верифікації моделей як ПКМ у цілому та і їх окремих компонентів, без застосування складних засобів μ -обчислень та позиційної динамічної логіки;*

у рамках виконаних досліджень щодо вибору засобів та методів захисту інформації в системах документообігу підприємств, отримано такі наукові результати:

- *розроблено метод інтелектуального розпізнавання загроз на основі дискретних процедур з використанням апарату логічних функ-*

цій та нечітких множин ознак НСД, що дозволяє створювати ефективні аналітичні, схемотехнічні та програмні рішення СЗІ;

- розроблено модель складання вирішального правила для дискретних процедур розпізнавання загроз ІБ, яка дозволяє виконувати інтелектуальне розпізнавання загрози, з мінімальним числом помилок;*
- модель інтелектуального розпізнавання загроз ІБ на основі мультимножин які інтерпретують нормальну і аномальну поведінку складної системи, що дозволяє оцінити оперативність і точність обробки даних в ІС в умовах навмисних впливів з боку порушників.*

СПИСОК ЛІТЕРАТУРНИХ ПЕРШОДЖЕРЕЛ

1. Іванілов, О. С. Економіка підприємства [Текст] : підруч. [для студ. вищ. навч. закл.] / О. С. Іванілов. — К. : Центр учбової літератури, 2009. — 728 с.
2. Доценко, Д. В. Экономическая безопасность: методологические аспекты и составляющие [Текст] / Д. В. Доценко, В. Н. Круглов // Аудит и финансовый анализ. — 2009. — № 4. — С. 415-427.
3. Логутова, Т. Г. Економічна безпека підприємства: сутність, завдання та методи забезпечення [Текст] / Т. Г. Логутова, Д. І. Нагаєвський // Теоретичні і практичні аспекти економіки та інтелектуальної власності. — 2011. — Т. 2. — С. 204-207.
4. Экономика и организация производства [Текст] : [учебн. пособ.] / под ред. Ю. И. Трещевского, Л. П. Пидоймо. — Воронеж : Воронежский гос. ун-т, 2010. — 854 с.
5. Овчаренко, Є. І. Система економічної безпеки підприємства: ознаки та принципи функціонування [Текст] / Є. І. Овчаренко // Економіка. Менеджмент. Підприємництво. — 2012. — № 24(II). — С. 133-143.
6. Іванюта, Т. М. Економічна безпека підприємства [Текст] : [навч. посіб. для студ. вищ. навч. закл.] / Т. М. Іванюта, А. О. Заїчковський. — К. : Центр учбової літератури, 2009. — 256 с.
7. Шпак, Н. О. Основні принципи формування стратегії забезпечення економічної стабільності підприємства [Електронний ресурс] / Н. О. Шпак, М. І. Романишин. — Режим доступу: \www/ URL: http://rusnauka.com/14_NPRT_2010/Economics/67034.doc.htm.
8. Череп, О. Г. Управління фінансово-економічною безпекою підприємств в Україні [Текст] / О. Г. Череп, З. П. Урусова, А. А. Урусов // Вісник ЖДТУ. Серія: Економічні науки. — 2012. — № 3(61). — С. 328-330.
9. Орлик О. В. Економічна безпека підприємства: властивості, стратегія та методи забезпечення [Текст] / О. В. Орлик // Економічна безпека в умовах глобалізації світової економіки : [колективна монографія у 2т.]. — Дніпропетровськ : «ФОРМ Дробязко С.І.», 2014. — Т. 2. — С. 176-182.
10. Островський, П. І. Аграрний маркетинг [Текст] : [навч. посіб.] / П. І. Островський. — К. : Центр навчальної літератури, 2006. — 224 с.
11. Экономика и организация безопасности хозяйствующих субъектов / [В. С. Гусев, Б. И. Кузин, М. Д. Медников и др.]. — СПб. : Очарованный странник, 2001. — 256 с. — ISBN 5-299-00119-3.
12. Мойсеєнко І. П. Управління фінансово-економічною безпекою підприємства [Текст] : навч. посібник / І. П. Мойсеєнко, О. М. Марченко. — Львів, 2011. — 380 с.

13. Якубович, З. Ідентифікація загроз економічній безпеці машинобудівного підприємства / З. Якубович // Галицький економічний вісник. — 2010. — №3 (28). — С. 107-112.
14. Доценко, І. О. Вплив внутрішніх та зовнішніх факторів загроз на рівень економічної безпеки підприємства / І. О. Доценко // Вісник ЖДТУ № 4 (54). — 2010. — С. 227-230.
15. Гинис, Л. А. Иерархическая структура системы экономической безопасности [Електронний ресурс] / Л. А. Гинис // Альманах современной науки и образования. — 2007. — № 4 (4). — С. 64-67. — Режим доступа : www.gramota.net/materials/1/2007/4/18.html
16. Ермолаев, Д. В. Угрозы экономической безопасности предприятия [Електронний ресурс] / Д. В. Ермолаев // Известия ТулГУ. Экономические и юридические науки. — Вып. 2. — Часть II. — С. 169-172. — Режим доступа : [http://publishing.tsu.tula.ru/izvest/tsu_izv_Ekonomich_i_uridicheskiye_nauki_2012_\(2_chast_2\).pdf#page=169](http://publishing.tsu.tula.ru/izvest/tsu_izv_Ekonomich_i_uridicheskiye_nauki_2012_(2_chast_2).pdf#page=169)
17. Гадышев, В. А. Классификация угроз экономической безопасности предприятия [Електронний ресурс] / В. А. Гадышев, О. Г. Поскочинова. — Режим доступа : <http://vestnik.igps.ru/wp-content/uploads/V32/6.pdf>
18. Васильців Т. Г., Пасічник М. Б. Чинники та джерела загроз економічній безпеці підприємства / Т. Г. Васильців, М. Б. Пасічник // Науковий вісник НЛТУ України: Збірник науково-технічних праць. — Вип. 18.10. — 2008. — С. 128-135.
19. Лянной, Г. Экономическая безопасность предприятия. Внешние и внутренние угрозы предпринимательской деятельности [Електронний ресурс] / Г. Лянной // Best of security. — 2006. — № 7. — Режим доступа : http://www.bos.dn.ua/view_article.php?id_article=27.
20. Орлик, О. В. Система загроз економічній безпеці суб'єктів господарювання [Текст] / О. В. Орлик // Вісник соціально-економічних досліджень : зб. наук. праць. — Одеса : ОНЕУ. — 2014. — Вип. 1(52). — С. 250-257. — ISSN 2313-4569.
21. Інтерв'ю Урядового уповноваженого Валерія Мунтіяна Українському національному агентству Укрінформ 15 січня 2013 року [Електронний ресурс] // Портал: Урядовий портал. — Режим доступа : \www/ URL: http://www.kmu.gov.ua/control/uk/publish/article?art_id=245972329. — Заголовок з екрану, доступ вільний, 27.02.2014.
22. Кракос Ю. Б. Управління фінансовою безпекою підприємств [Текст] / Ю. Б. Кракос, Р. О. Разгон // Економіка та управління підприємствами машинобудівної галузі: проблеми теорії та практики. — 2008. — № 1(1). — С. 86-97.
23. Фінансово-економічна безпека підприємств України: стратегія та механізми забезпечення [Текст] : монографія / Т. Г. Васильців, В. І.

- Волошин, О. Р. Бойкевич, В. В. Каркавчук ; за ред. Т. Г. Васильціва. — Львів : Ліга-Прес, 2012. — 386 с.
24. Орлик, О. В. Фінансово-економічна безпека підприємства та підходи до її забезпечення [Електронний ресурс] / О. В. Орлик // Інформаційна та економічна безпека : міжнар. наук.-практ. конф., 2014 р. : матер. конф. ¼ X. : ХІБС УБС НБУ. — 1 електрон. опт. диск (CD-ROM). — Систем. вимоги: Pentium ; 512 Mb RAM ; Windows XP, 7, 8 ; Adobe Acrobat Reader 5.0-10.0. — Назва з екрану.
25. Лазаренко М. П. Фінансова безпека підприємства та її управління [Електронний ресурс] / М. П. Лазаренко, К. В. Ніколаєнко. — Режим доступу : [\www/ URL: http://rusnauka.com/1_KAND_2010/Economics/10_57970.doc.htm](http://www.rusnauka.com/1_KAND_2010/Economics/10_57970.doc.htm). — Заголовок з екрану, доступ вільний, 27.02.2014.
26. Орлик, О. В. Економічна безпека господарюючих суб'єктів муніципального утворення [Текст] / О. В. Орлик // Удосконалення принципів та методів інформаційного забезпечення, інформаційної та фінансово-економічної безпеки підприємств та організацій сфери економіки, бізнесу та фінансів : звіт про НДР. ¼ Одеса : ОНЕУ, 2013. ¼ С. 87-97.
27. Клименко Т. В. Основні елементи механізму забезпечення фінансової безпеки суб'єктів господарювання [Текст] / Т. В. Клименко // Вісник ЖДТУ. Серія: Економічні науки. — 2011. — № 4(58). — С. 340-343.
28. Убытки от утечек информации возросли на 25% в 2013 году [Електронний ресурс]. — Режим доступу : [\www/ URL: http://ubr.ua/market/media-market/ubytki-ot-utechek-informacii-vozrosli-na-25-v-2013-godu-280557](http://ubr.ua/market/media-market/ubytki-ot-utechek-informacii-vozrosli-na-25-v-2013-godu-280557). — Заголовок з екрану, доступ вільний, 27.02.2014.
29. Орлик О. В. Методи управління фінансово-економічною безпекою [Текст] / О. В. Орлик // Сборник научных трудов SWorld. — Иваново : МАРКОВА АД, 2014. — Т. 28. — Вып. 1. — С. 37-41. — ISSN 2224-0187.
30. Орлик, О. В. Напрямки формування надійної системи економічної безпеки суб'єктів господарювання [Текст] / О. В. Орлик // Соціально-економічні аспекти розвитку економіки та управління : міжнар. наук.-практ. конф., 16-17 січня 2014 р. : матер. конф. — Дніпропетровськ : «ФОП Дробязко С.І.». — С. 306-309.
31. Гончаренко, Л. П. Процесс обеспечения экономической безопасности предприятия [Електронний ресурс] / Л. П. Гончаренко // Справочник экономиста. — 2004. — №12. — Режим доступу : http://www.profiz.ru/se/12_2004/952
32. Orlyk, O. V. Financial and economic security of the enterprise and principles of its provision / O. V. Orlyk // Economics and management : theory and practice: Collection of scientific articles. Vol. 2. — Verlag SWG imex GmbH, Nürnberg, Deutschland, 2014. — P. 286-291.

33. Орлик, О. В. Інформаційні системи як стратегічній засіб розвитку фірми [Текст] / О. В. Орлик, О. Г. Єсіна // Вісник соціально-економічних досліджень. — 2001. — № 10. — С. 386-390.
34. Коробчинський, О. Л. Методика формування системи економічної безпеки підприємства [Текст] / О. Л. Коробчинський // Актуальні проблеми економіки. — №4 (94). — 2009. — С. 41-45.
35. Орлик, О. В. Сучасні інформаційні технології в системі управління підприємством [Текст] / О. В. Орлик, О. Г. Єсіна // Вісник соціально-економічних досліджень. — 2002. — № 11. — С. 293-296.
36. Линниченко, А. Проблемы безопасности предпринимательской деятельности. Суть проблемы обеспечения безопасности предпринимательской деятельности [Электронный ресурс] / Портал: Медиапортал о безопасности. — Режим доступа \www/ URL: http://www.psj.ru/saver_people/detail.php?ID=64652 — Заглавие с экрана, доступ свободный, 03.10.2012.
37. Прасолов, В. Современные аспекты экономической безопасности [Электронный ресурс] / Портал: Bos est of Security. — Режим доступа \www/ URL: http://www.bos.dn.ua/view_article.php?id_article=46 — Заглавие с экрана, доступ свободный, 02.10.2012.
38. Сесин, Е. М. Построение моделей идентификации личности, основанных на сравнении множества физических или поведенческих характеристик человека [Текст] / Е. М. Сесин, В. М. Белов // Вестник СибГУТИ. — 2011. — №4. — С. 41-50. — ISSN 1998-6920.
39. Ушмаев, О. С. Информационная технология интеграции идентификации по изображению лица для ускорения автоматической дактилоскопической идентификации [Текст] / О. С. Ушмаев // Информатика и ее применения. — 2008. — №4. — Т. 2. — С. 66-73. — ISSN 1992-2264.
40. Neyman, J. On the problem of the most efficient tests of statistical hypotheses [Текст] / J. Neyman, E. S. Pearson // Philos. Trans. R. Soc. — 1993. — №231. — P. 289 -337. — ISSN 0962-8436.
41. Phillips, P. Facial recognition vendor test 2002 : Evaluation report, March 2003 [Електронний ресурс] / P. Phillips, P. Grother, R. Micheals, D. Blackburn, E. Tabassi, M. Bone // Портал : frvt.org. — Режим доступу \www/ URL: <http://www.frvt.org>. — Заголовок з екрану, доступ вільний, 16.02.2014.
42. Ushmaev, O. S. Problems of automatic fusion of biometric identifiers [Текст] / O. S. Ushmaev // Pattern Recognition and Image Analysis. — 2009. — V.19. — №3. — P. 534-538. — ISSN 1054-6618.
43. Пахомов, С. Отпечаток пальца вместо пароля [Текст] / С. Пахомов // Компьютер-Пресс. — 2004. — №4. — ISSN 0868-6157 : [Електронний ресурс] // Портал : Компьютер-Пресс. — Режим доступу \www/ URL: <http://compress.ru/Archive/CP/2004/4/11/>. — Заголовок з екрану, доступ вільний, 17.02.2014.

44. Гусев, Г. А. Под мультибиометрическим контролем [Текст] / Г. А. Гусев // Системы безопасности. — 2009. — №3. — С. 134-136. — ISSN відсутній.
45. Грузман, И. С. Цифровая обработка изображений в информационных системах : навчальний посібник / И. С. Грузман, В. С. Киричук, В. П. Косых [та ін.] // Новосибирск : НГТУ, 2002. — 352 с.
46. Казакова, Н. Ф. Синтез методу виділення контурів у системах ідентифікації на основі усереднення перепадів яскравості [Текст] / Н. Ф. Казакова, О. О. Фразе-Фразенко // Інформаційна безпека. — 2013. — №2(10). — С.48-57. — ISSN 2224-9613.
47. Вакуленко, А. Биометрические методы идентификации личности: обоснованный выбор и внедрение [Электронный ресурс] / А. Вакуленко, А. Юхнин // Портал : НПО ИНФОРМ: Биометрические системы безопасности. — Режим доступа \www/ URL: <http://www.proinform.com/press/biovybor/>. — Заголовок з екрану, доступ вільний, 17.02.2014.
48. Phillips, P. Facial recognition vendor test 2002: Evaluation report [Електронний ресурс] / P. Phillips, P. Grother, R. Micheals, D. Blackburn [и др.] // Портал : frvt.org. — Режим доступа \www/ URL: <http://www.frvt.org/>. — Заголовок з екрану, доступ вільний, 17.02.2014.
49. Фразе-Фразенко, А. А. Система текстурных признаков, основанных на измерении пространственных частот [Текст] / А. А. Фразе-Фразенко // Технологічний аудит та резерви виробництва. — 2013. — №5/5(13). — С. 60-62.
50. Griffin, P. Topics for multi-biometric research «MMUA-2003» : Panel Discussion [Електронний ресурс] / P. Griffin // Портал : без назви. — Режим доступа \www/ URL: <http://mmuaxs.ucsb.edu/>. — Заголовок з екрану, доступ вільний, 19.02.2014.
51. Bonsor, K. How Facial Recognition Systems Work [Електронний ресурс] / K. Bonsor, R. Johnson // Портал : Howstuffworks — Режим доступа \www/ URL: <http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm>. — Заголовок з екрану, доступ вільний, 15.01.2013.
52. Скопа О. О., Фразе-Фразенко О. О. Анізотропна фільтрація зображень у системах аутентифікації // Матеріали II Міжнар. наук.-техн. конф. «Захист інформації і безпека інформаційних систем», Львів, 30 травня — 01 червня 2013 р. — Львів : НУ «Львівська політехніка», 2013. — С. 156-158.
53. Фразе-Фразенко, А. А. Система текстурных признаков, основанных на измерении пространственных частот [Текст] / А. А. Фразе-Фразенко // Технологічний аудит та резерви виробництва. — 2013. — №5/5(13). — С. 60-62. — ISSN 2226-3780.
54. Казакова, Н. Ф. Исследование и применение в системах защиты информации корреляционного критерия сходства графических структур

- [Текст] // Информационные системы в управлении, образовании, промышленности : монография / Н. Ф. Казакова, А. А. Фразе-Фразенко [и др.] ; под ред. В. С. Пономаренко. — Х. : ТОВ «Щедра садиба плюс», 2014. — 498 с. (Русск. яз.). — ISBN 978-617-7188-50-5.
55. Фразе-Фразенко, О. О. Огляд та аналіз поточного стану технологій розпізнавання образів та перспективи їх використання у системах захисту інформації // Удосконалення принципів та методів інформаційного забезпечення, інформаційної та фінансово-економічної безпеки підприємств та організацій сфери економіки, бізнесу та фінансів [Звіт про НДР] : (проміжн.) / О. О. Скопа, Н. Ф. Казакова, О. В. Орлик, Ю. В. Щербина, А. О. Петров, С. Л. Волков, О. І. Мацків, О. Г. Єсіна, А. Ю. Вакула, О. О. Фразе-Фразенко, А. В. Мінін, О. О. Йона, Є. В. Вавілов, К. Б. Айвазова ; кер. О. О. Скопа. — Одеса : ОНЕУ, 2013. — 0112U007713. — 236 с. — С. 38-69.
 56. Мак-Каллок, У. С. Логическое исчисление идей, относящихся к нервной активности [Текст] / У. С. Мак-Каллок, В. Питтс // Нейрокомпьютер. — 1992. — №3. — С. 39-53.
 57. Скопа, О. О. Глобальні властивості нейронних мереж [Текст] / О. О. Скопа, Н. Ф. Казакова // Наукові записки УНДІЗ. — 2008. — №3(5). — С.13-19.
 58. Дрейфус, У. Чего не могут вычислительные машины: Критика искусственного разума : монография / Переклад с англ. Н. Родмана ; під ред. Б. В. Бірюкова. — М. : Прогресс, 1978. — 334 с.
 59. Скопа, А. А. Нейронна мережа як об'єкт техносфери: властивості [Текст] / А. А. Скопа, Н. Ф. Казакова // Наукові записки Міжнародного гуманітарного університету. — Одеса : МГУ. — 2008. — №11 : Управління проектами та програмами ; відп. за випуск А. І. Рибак. — С.44-48.
 60. McCarthy J. What is Artificial Intelligence? [Электронный ресурс] // Портал : без назви. — Режим доступа \www/ URL : <http://www-formal.stanford.edu/jmc/whatisai.html>. — Заголовок з екрану, доступ вільний, 13.01.2010.
 61. Минский, М. Перцептроны : монография / М. Минский, С. Пейперт // Переклад з англ. Г. Л. Гімельфарба та В. М. Шарипанова ; під ред. В. А. Ковалевського. — М. : Мир, 1977. — 262 с.
 62. Скопа, О. О. Концептуальні положення створення нейронних мереж в Україні [Текст] / О. О. Скопа // Наукові записки УНДІЗ. — 2008. — №1(3). — С.3-19.
 63. Скопа, О. О. Наукова концепція інтелектуальної мережі [Текст] / О. О. Скопа // Наукові записки Міжнародного гуманітарного університету. — 2008. — С. 44-49.
 64. Вилли, К. Биология: Биологические процессы и законы : монография / К. Вилли, В. Детье. — М. : Мир, 1975. — 822 с.

65. Скопа, О. О. Нейронна мережа як об'єкт техносфери: концептуальні положення створення [Текст] / О. О. Скопа, Н. Ф. Казакова // Наукові записки Міжнародного гуманітарного університету. — Одеса : МГУ. — №10 : Управління проектами та програмами ; відп. за випуск А. І. Рибак. — С. 44-60.
66. Баховський, П. Ф. Концептуальні положення створення та розвитку інтелектуальних мереж: Основоположні зауваження [Текст] / П. Ф. Баховський, О. О. Скопа // Моделювання та інформаційні технології. — К. : ІПМЕ НАН України. — 2008. — №49. — С. 154-159.
67. Кемп, П. Введение в биологию : монографія / П. Кемп, К. Арме. — М. : Мир, 1988. — 671 с.
68. Блум, Ф. Мозг, разум и поведение : монографія / Ф. Блум, А. Лейзерсон, Л. Хофстедтер. — М. : Мир, 1988. — 248 с.
69. Веккер, Л. М. Психика и реальность: Единая теория психических процессов : монографія / Л. М. Веккер. — М. : Смысл; PerSe, 2000. — 685 с.
70. Годфруа, Ж. Что такое психология / Ж. Годфруа. — М. : Мир, 1992. — Т. 1. — 496 с. — ISBN відсутній.
71. Выготский, Л. С. Психология : підручник / Л. С. Выготский. — М. : ЭКСМО-Пресс, 2000. — 1008 с.
72. Нормативний документ : НД ТЗІ 1.1-003-99 ДСТСЗІ СБ України «Системи технічного захисту інформації. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» [Текст] / Наказ ДСТСЗІ СБ України від 28 квітня 1999 року № 22. — Київ. — 1999.
73. Скопа, О. О. Вибір методики та розрахунок коефіцієнтів помилкового пропуску та помилкової відмови доступу у системах біометричної ідентифікації [Текст] / О. О. Скопа, О. О. Фразе-Фразенко // Бионика интеллекта. — 2014. - № 1(82). — С. 80-89.
74. Нормативний документ : ГОСТ Р ИСО/МЭК 7498-1-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель [Текст]. — Введ. 01.01.2000. — М. : Федеральное агентство по стандартизации и метрологии ; [Электронный ресурс] // Портал : gost.ru. — Режим доступа \www/ URL: <http://protect.gost.ru/v.aspx?control=7&id=132355>. — Заголовок з екрану, доступ вільний, 18.05.2013.
75. Скопа, О. О. Показники якості та життєві цикли захищених інформаційно-вимірювальних систем [Текст] / О. О. Скопа, С. Л. Волков, О. В. Грабовський // Вісник Східноукраїнського національного університету імені Володимира Даля. — 2013. - № 15(204). — Ч. 1. — С. 192-198.
76. Скопа, О. О. Проблематика якості послуг інтернет-провайдерів [Текст] / О. О. Скопа, С. Л. Волков, К. Б. Айвазова // Збірник наукових праць Одеської державної академії технічного регулювання та якості. — 2013. - № 1(2). — С. 27-31.

77. Грабовський, О. В. Регуляризація визначення показників якості функціонування ІВС з врахуванням нечіткості інформації [Текст] / О. В. Грабовський, С. Л. Волков, О. О. Скопа // Вісник Національного технічного університету «ХПІ». – 2013. - № 26(999). – С. 169-174.
78. Грабовський, О. В. Візуалізація структури показників якості інформаційно-вимірювальних систем [Текст] / О. В. Грабовський, С. Л. Волков, О. О. Скопа // Метрологія та прилади. – 2013. - № 2(40). – С. 69-74.
79. Skopa, O. O. Theoretical researches of smart antennas [Текст] / O. O. Skopa // Інформаційна безпека. – 2012. - № 2(8). – С. 136-143.
80. Болдарев, А. Г. Реализация программной закладки методом прямого доступа к устройствам ввода raw input api [Текст] / А. Г. Болдарев, А. А. Петров, А. А. Скопа // Інформаційна безпека. – 2012. - № 2(8). – С. 13-22.
81. Скопа, О. О. Безпека фінансового ринку та фінансової стабільності як суспільне благо [Текст] / О. О. Скопа, О. О. Йона // Вчені записки університету «КРОК». – 2012. – № 32. – Т. 1. – С. 117-122.
82. Волков, С. Л. Алгоритм тактової синхронізації цифрового радіомодема на основі ШПФ [Текст] / С. Л. Волков, О. О. Скопа // Вісник Національного технічного університету «ХПІ». – 2012. - № 44(950). – С. 61-66.
83. Петров, А. О. Використання сигналоподібних завад у системах активного захисту інформації [Текст] / А. О. Петров, О. В. Рибальський, О. О. Скопа, В. О. Хорошко // Сучасна спеціальна техніка. – 2012. - № 1(28). – С. 69-75.
84. Скопа, О. О. Аспекти безпеки протоколу FTP [Текст] / О. О. Скопа // Інформаційна безпека. – 2012. - № 1(7). – С. 96-103.
85. Мінін, А. В. Біноміальні моделі випробування живучості захищених інформаційних каналів [Текст] / А. В. Мінін, О. О. Скопа, М. Александер // Вісник Східноукраїнського національного університету імені Володимира Даля. - 2012. - № 8(179). - Ч. 1. – С. 42-58.
86. Скопа, О. О. Комплексна протидія вразливостям протоколу FTP [Текст] / О. О. Скопа, Л. Т. Пархуць // Наукові записки УНДІЗ. – 2012. - № 1(21). – С. 26-32.
87. Скопа, О. О. Проектний аналіз узгодження вимог до надійності при впровадженні організаціями комунікаційних профілактичних заходів [Текст] / О. О. Скопа, С. А. Лисюк, А. В. Мінін // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – 2011. – № 33. – С. 122-128.
88. Скопа, О. О. Інструментальні засоби статистичного тестування криптографічних перетворень [Текст] / Скопа О.О. // Вісник Національного технічного університету «ХПІ». – 2011. - № 33. – С. 77-83.

89. Скопа, О. О. Обчислення аперіодичної автокореляційної функції та визначення критеріїв її якості по В. П. Іпатову [Текст] / Скопа О.О. // Інформаційна безпека. - 2011. - № 1(5). - С. 146-153.
90. Скопа, О. О. Синтез адаптивного приймача цифрового сигналу для інформаційних радіосистем підвищеної надійності [Текст] / Скопа О.О. // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2011. - № 7(161). – Ч. 1. - С. 21-27.
91. Скопа, А. А. Факторизация модели отказа в мультисервисной телекоммуникационной сети на уровне управления услугами [Текст] / А. А. Скопа, Н. М. Билык // Інформаційна безпека. - 2010. - № 2(4). - С. 132-139.
92. Скопа, А. А. Принципиальная задача анализа и синтеза стохастической модели отказов обслуживания в сетях новых поколений на уровне опорной коммутации и уровне доступа к среде передачи [Текст] / Скопа А.А., Гринь В.А. // Інформаційна безпека. - 2010. - № 1(3). - С. 131-137.
93. Панфилов, В. И. Синтез частотных цифровых приемников для защищенных радиосистем [Текст] / В. И. Панфилов, А. А. Скопа // Вісник ДУИКТ. - 2009. - №4. - Т. 7. - С. 361-369.
94. Гундериц, Г. А. Прогностические модели факторов отказов современных телекоммуникационных сетей и сетей NGN [Текст] / Г. А. Гундериц, Н. А. Одегов, А. А. Скопа // Радіотехніка. – 2009. - № 159. – С. 24-29.
95. Гура, В. И. Предложения по модернизации стандарта IEEE 802.11 с целью повышения защищенности информации [Текст] / В. И. Гура, А. А. Скопа, А. А. Сыропятов // Інформаційна безпека. – 2009. - № 2. - Т.2. - С. 136-139.
96. Білик, Н. М. Аналіз моделей первинних датчиків псевдовипадкових чисел [Текст] / Н. М. Білик, О. О. Скопа // Системи обробки інформації. – 2009. - № 7(79). – С. 56-59.
97. Скопа, О. О. Аналіз розвитку сучасних напрямів інформаційної безпеки автоматизованих систем [Текст] / О. О. Скопа, Н. Ф. Казакова // Системи обробки інформації. – 2009. - № 7(79). – С. 48-54.
98. Согіна, Н. М. Методика біноміальних випробувань об'єктів одноразового використання [Текст] / Н. М. Согіна, О. О. Скопа, В. В. Мірошников, Я. І. Торощанко // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – 2009. – № 21. – С. 120-128.
99. Панфилов, В. И. Синтез помехоустойчивых модемов при совместном воздействии в канале аддитивных шумов и преднамеренных помех [Текст] / В. И. Панфилов, А. А. Скопа // Наукові записки УНДІЗ. – 2008. - № 6(8). – С. 72-80.

100. Щербина, Ю. В. Проблемы оценки защищенности автоматизированных систем [Текст] / Ю. В. Щербина, А. А. Скопа // Захист інформації. – 2008. - № 4(41). – С. 23-29.
101. Скопа, О. О. Знаходження g -нижньої границі показника надійності системи з m послідовно з'єднаних об'єктів за результатами їх автономних біноміальних випробувань [Текст] / О. О. Скопа, Г. А. Гундерич // Наукові записки УНДІЗ. – 2008. – № 5(7). – С. 73-77.
102. Скопа, О. О. Оцінка надійності систем телекомунікацій з послідовним з'єднанням об'єктів за результатами їх біноміальних іспитів з зупинкою [Текст] / О. О. Скопа, В. Г. Головань // Наукові записки УНДІЗ. – 2008. – № 4(6). – С. 75-79.
103. Скопа, А. А. Анализ методов исследования замираний [Текст] / А. А. Скопа, Н. М. Билык // Радиотехника. – 2007. – № 151. – С. 177-180.
104. Казакова, Н. Ф. Принципи побудови захищених інтелектуальних мереж [Текст] / Н. Ф. Казакова // Вісник ДУІКТ. — К. : ДУІКТ. — 2009. — № 4. — Т. 7. — С. 381-388.
105. Казакова, Н. Ф. Доповнення до концепції інформаційної безпеки [Текст] / Н. Ф. Казакова // Сучасна спеціальна техніка. — К. : Державний науково-дослідний інститут МВС України. — 2010. — № 3(22). — С. 74-80.
106. Скопа, А. А. Прикладное применение уравнений Клоппера-Пирсона в системах телекоммуникаций [Текст] / А. А. Скопа, К. Б. Никифоренко, Н. М. Согина // Наукові записки УНДІЗ. – 2007. - № 2. – С. 83-88.
107. Кобозева, А. А. Стеганографический метод обеспечения информационной безопасности морской связи [Текст] / А. А. Кобозева, И. И. Маракова, А. А. Скопа // Збірник наукових праць НУК. – 2006. – № 3(408). – С. 155–161.
108. Скопа, О. О. Перспективи використання ґратчастого кодування в інформаційних радіосистемах з корелятивною обробкою сигналу [Текст] / О. О. Скопа, Я. І. Торошанко, К. Б. Нікіфоренко // Збірник наукових праць ІПМЕ. – 2006. – № 35. – С. 49-55.
109. Дакдуки, А. С. Информационно-теоретическое обоснование для смарт-антенн [Текст] / А. С. Дакдуки, Н. К. Михайлов, В. Л. Банкет, А. А. Скопа // Праці УНДІРТ. – 2004. – № 2(38). – С. 11-15.
110. Скопа, О. О. Плани проведення випробувань надійності систем телекомунікацій з накопиченням пошкоджень [Текст] / О. О. Скопа // Праці УНДІРТ. – 2003. – № 3(35). – С. 104-106.
111. Skopa O. Task of redundancy optimization // Proceedings of the VIIIth International Conference CADSM'2003 «The Experience of Designing and Application of CAD Systems of Microelectronics»: February 18-23, 2003. - Lviv-Slavske, Ukraine: Lviv Polytechnic National University - IEEE Networking the World. - 2002. - С. 330.

112. Скопа О.О. Однобічна процедура контролю надійності резервних каналів зв'язку / Наук. праці ДонДТУ. Серія: Обчислювальна техніка та автоматизація. Випуск 47. – Донецьк: РВА ДонДТУ, 2002. - С. 168-175.
113. Skopa O. Construction of the System of Radio Communication Network Management // Proceeding of the International Conference TCSET'2002 «Modern Problems of Radio Engineering, Telecommunications and Computer Science»: February 18-23, 2002. - Lviv-Slavsk, Ukraine: Lviv Polytechnic National University - IEEE Networking the World. - 2002. - С. 285.
114. Скопа, О. О. Управління відносною ефективною швидкістю передачі в мережах з комутацією пакетів [Текст] / О. О. Скопа, В. В. Корчинський // Вісник Національного університету «Львівська політехніка». - 2002. - № 443. - С. 75-80.
115. Скопа, О. О. Побудова систем мережного управління радіозв'язком [Текст] / О. О. Скопа // Вісник Національного університету «Львівська політехніка». - 2002. - № 443. - С. 81-85.
116. Мазурков, М. И. Свойства циклических по времени частотно-временных кодов кубических вычетов над расширенными полями Галуа [Текст] / М. И. Мазурков, А. А. Скопа // Информатика и связь. – 1997. – С. 201-209.
117. Цифрова обробка аудіо- та відеоінформації у мультимедійних системах : підручник для вищих навчальних закладів [Текст] / П. Ф. Олексенко, В. В. Коваль, В. С. Лазебний, Г. М. Розорінов, О.О. Скопа [за ред. акад. НАН України В.Ф. Мачуліна]. – К. : Наукова думка, 2014. – 152 с.
118. Основы компьютерной графики : учебное пособие [Текст] / С. Л. Емельянов, А. А. Скопа, А. Б. Козин. – О. : Феникс, 2007. – 188 с.
119. Протоколи міжмережної взаємодії : навчальний посібник [Текст] / П. П. Воробієнко, В. В. Каразей, О. О. Скопа. – Одеса : УДАЗ ім.О.С.Попова, 1999. – 50 с.
120. Практичні системи зв'язку з шумоподібними сигналами : навчальний посібник [Текст] / М. І. Мазурков, О. О. Скопа. – Одеса : Фотосинтетика, 2001. - 62 с.
121. Современные системы телекоммуникаций : учебное пособие [Текст] / М. И. Мазурков, П. Е. Баранов, И. Н. Еримичой, А. А. Скопа, В. Б. Ткаченко, В. Я. Чечельницкий [под ред. М. И. Мазуркова]. – Одесса : Од-ГПУ, 2001. – 280 с. : ил. 126.
122. Практичне введення в Інтернет : навчальний посібник [Текст] / В. В. Корчинський, Л. А. Нікітюк, О. О. Скопа. – Одеса : ОНАЗ ім. О. С. Попова, 2001. – 44 с.
123. Програмування на алгоритмічній мові Pascal : навчальний посібник [Текст] / О. О. Скопа. - Одеса : Міжнар. гуманіт. ун-т, 2004. – 67 с.

124. Казакова, Н. Ф. Дослідження та застосування в системах захисту інформації кореляційного критерію подібності графічних структур [Текст] / Н. Ф. Казакова, О. О. Фразе-Фразенко // Проблемы и перспективы развития ИТ-индустрии : VI Міжнар. наук.-практ. конф., 17-18 квітня 2014 р. : матер. конф. — Харківський національний економічний університет ім. Семена Кузнеця, Харків. — С. 246.
125. Казакова, Н. Ф. Дослідження та застосування в системах захисту інформації кореляційного критерію подібності графічних структур [Текст] / Н. Ф. Казакова, О. О. Фразе-Фразенко // Системи обробки інформації. — 2014. — № 2(118). — Т. 2 : Проблеми і перспективи розвитку ІТ-індустрії. — С. 246.
126. Безпека банківської діяльності : монографія [Текст] / Н. Ф. Казакова, В. І. Панфілов, Л. М. Скачек, О. О. Скопа, В. О. Хорошко ; за ред. проф. Хорошко В. О. — К. : ПВП «Задруга», 2013. — 282 с.
127. Основи лінійного програмування : навчальний посібник [Текст] / С. К. Варбанець, О. О. Скопа. — Одеса : Неогоціант, 2005. — 53 с.
128. Казакова, Н. Ф. Алгоритм розрахунку надійності комп'ютерних пристроїв управління резервом на основі напівмарківських процесів [Текст] / Н. Ф. Казакова // Радиоэлектроника и молодежь в XXI веке : IX Міжнар. молод. форум, 19-21 квітня 2005 р.: зб. наук. праць. — ХТУРЕ, Харків. — С. 111.
129. Казакова, Н. Ф. Використання НМ-процесів при аналізі функціонування пристроїв управління резервним обладнанням [Текст] / Н. Ф. Казакова // Питання розвитку телекомунікаційних мереж : наук.-навч. семін., 8-9 червня 2006 р. : матер. семін. — УНДІЗ, Київ. — С. 11-19.
130. Казакова, Н. Ф. Оптимізація стратегії обслуговування резервних систем зв'язку [Текст] / Н. Ф. Казакова // Вісник УБЕНТЗ. — 2002. — № 2. — С. 79-80.
131. Казакова, Н. Ф. Особенности расчета показателей надежности компьютерных устройств управления резервным оборудованием [Текст] / Н. Ф. Казакова // Системний аналіз та інформаційні технології : VI Міжнар. наук.-практ. конф. студентів, аспірантів та молодих вчених ІПСА-2004, 1-3 липня 2004 р. : матер. конф. — НТУУ «КПІ», Київ. — С. 209-210.
132. Казакова, Н. Ф. Порівняння методів управління вибором резервного радіоканалу [Текст] / Н. Ф. Казакова // Праці УНДІРТ. — 2002. — № 1(29). — С. 49-51.
133. Казакова, Н. Ф. Стратегії заміни елементів у системах телекомунікацій з резервом [Текст] / Н. Ф. Казакова // Системи и средства передачи и обработки информации : VI Міжнар. наук.-практ. конф., 3-8 вересня 2002 р. : матер. конф. — ОНАС ім. О. С. Попова, Одеса. — С. 42-43.
134. Казакова, Н. Ф. Задача управління оптимальним резервуванням в багатоканальних інформаційних системах [Текст] / Н. Ф. Казакова, Н. М.

- Білик // Наукові записки Міжнародного гуманітарного університету. — 2008. — № 13. — С. 104-108.
135. Казакова, Н. Ф. Методи оцінки надійності систем телекомунікацій з резервом [Текст] / Н. Ф. Казакова // Праці УНДІРТ. — 2003. — № 2(34). — С. 109-112.
136. Скопа, О. О. Вплив функціональної надмірності резервованих систем телекомунікацій на скорочення обсягів їх випробувань на надійність [Текст] / О. О. Скопа, Н. Ф. Казакова, О. С. Мурін // Наукові праці Донецького національного технічного університету. — 2003. — № 58. — С.115-121.
137. Казакова, Н. Ф. Принциповий аспект при випробуваннях живучості систем критичного застосування за біноміальною схемою Бернуллі [Текст] / Н. Ф. Казакова // Технологічний аудит та резерви виробництва. — 2012. — № 6/3(8). — С. 25-27.
138. Казакова, Н. Ф. Скорочення обсягу випробувань систем телекомунікацій на надійність за рахунок їх структурної надмірності [Текст] / Н. Ф. Казакова, О. М. Мухін, О. О. Скопа // Прикладная радиоэлектроника. Состояние и перспективы развития : I Міжнар. радіоелектрон. форум, 8-10 жовтня 2002 р. : сб. наук. праць. — ХНУ-РЭ, Харків. — С. 358-360.
139. Казакова, Н. Ф. Аспекти надійної роботи автоматичних систем з послідовно-паралельним з'єднанням резервуючих елементів [Текст] / Н. Ф. Казакова // Вісник національного університету «Львівська політехніка». — 2012. — № 738. — С. 235-245.
140. Овчаренко, В. В. Скорочення обсягу випробувань систем телекомунікацій за рахунок їх структурної надмірності [Текст] / В. В. Овчаренко, О. О. Скопа // Наукові записки Міжнародного гуманітарного університету. - 2005. - № 3. - С. 117-119.
141. Казакова, Н. Ф. Новий метод аналого-цифрового радіомовлення [Текст] / Н. Ф. Казакова // Технологічний аудит та резерви виробництва. — 2013. — № 1/1(9). — С. 19-22.
142. Спосіб сумісного аналого-цифрового мовлення у діапазоні ДВЧ [Текст] : пат. 77288 Україна : МПК Н 04J 1/00 / Балан М. М., Дмітрієва І. Ю., Іскендерзаде Ш. Г., Казакова Н. Ф. ; заявник та патентообладач ОНАЗ ім. О. С. Попова ; заявл. 10.07.2012 ; опубл. 11.02.2013, бюл. № 2.
143. Передавальний тракт аналого-цифрового радіомовлення у діапазоні ДВЧ [Текст] : пат. 89969 Україна : МПК Н 04J 1/00 / Балан М. М., Казакова Н. Ф., Вавілов Є. В., Іскендерзаде Ш. Г. ; заявник та патентообладач ОНАЗ ім. О. С. Попова ; заявл. 11.11.2013 ; опубл. 12.05.2014, бюл. № 9.
144. Казакова, Н. Ф. Розвиток теорії напівстохастичних матриць [Текст] / Н. Ф. Казакова // Технологічний аудит та резерви виробництва. — 2012. — № 5/2(7). — С. 31-32.

145. Грабовський, О. В. Скорочення випробувань надійності ІВС за рахунок її функціональної надмірності [Текст] / О. В. Грабовський, Н. Ф. Казакова // Технологічний аудит та резерви виробництва. — 2013. — № 2/1(10). — С. 24-27.
146. Скопа, О. О. Обслуговування резервних систем зв'язку [Текст] / О. О. Скопа // Наукові праці Донецького державного технічного університету. — 2002. — № 38. — С. 89-91.
147. Білик, Н. М. Скорочення обсягу профілактичних вимірювань в інформаційних мережах за рахунок їх структурної надмірності [Текст] / Н. М. Білик // Восточно-Европейский журнал передовых технологий. — 2010. — № 5/2(47). — С. 4-6.
148. Скопа, О. О. Принципи оптимального резервування в інформаційних мережах [Текст] / О. О. Скопа, К. Б. Нікіфоренко // Вісник УБЕНТЗ. — 2006. — №2. — С. 47-51.
149. Скопа, О. О. Нейронна мережа як об'єкт техносфери: концептуальні положення створення [Текст] / О. О. Скопа, Н. Ф. Казакова // Наукові записки Міжнародного гуманітарного університету. - 2008. - № 10. — С. 44-60.
150. Модельный закон : Об информатизации, информации и защите информации [Електронний ресурс] : міжнародний документ / Портал : rada.gov.ua. — Режим доступу \www/ URL: http://zakon0.rada.gov.ua/laws/show/997_d09. — Заголовок з екрану, доступ вільний, 29.07.2013.
151. Про телекомунікації : Закон України від 18 листопада 2003 року № 1280-IV [Текст] / Відомості Верховної Ради України. — 2004. — № 12. — С. 155. — [Поточна редакція від 19 квітня 2014 року].
152. Про інформацію : Закон України від 17 січня 2002 року № 2657-XII [Текст] / Відомості Верховної Ради України. — 1992. — № 48. — С. 650. — [Поточна редакція від 02 березня 2014 року].
153. Скопа, А. А. Нейронна мережа як об'єкт техносфери: властивості [Текст] / А. А. Скопа, Н. Ф. Казакова // Наукові записки Міжнародного гуманітарного університету. - 2008. - № 11. — С. 44-48.
154. Баховський, П. Ф. Концепція та сценарії реалізації віртуального домашнього оточення в мережах 3G [Текст] / П. Ф. Баховський, О. О. Скопа // Наукові записки Міжнародного гуманітарного університету. - 2008. - № 13. — С. 88-96.
155. Скопа, О. О. Дослідження методів оптимального резервування в телекомунікаціях [Текст] / О. О. Скопа, К. Б. Нікіфоренко // Вісник УНДІЗ. — 2008. - № 1. — С. 41-45.
156. Маракова, И. И. Защита информации в беспроводных информационных сетях [Текст] / И. И. Маракова, А. А. Скопа, А. А. Сыропятов // Вісник УНДІЗ. — 2008. - № 1. — С. 47-49.

157. Казакова, Н. Ф. Повышение адаптивности и достоверности вероятностной модели оценки живучести системы защиты шифрования [Текст] / Н. Ф. Казакова, Е. О. Тискина, В. А. Хорошко // Інформаційна безпека. — 2009. — № 2(2). — С. 69-73.
158. Казакова, Исследование информационных потоков в комплексных системах защиты информации и метод расчета пропускной способности [Текст] / Н. Ф. Казакова, Е. О. Тискина, В. А. Хорошко // Інформаційна безпека. — 2009. — № 2(2). — С. 105-115.
159. Казакова, Н. Ф. Визначення показників для вирішення завдань прогностичного контролю мультисервісних телекомунікаційних мереж [Текст] / Н. Ф. Казакова, О. О. Скопа // Сучасний захист інформації. — 2010. — Спецвипуск (4). — С. 55-61.
160. Казакова, Н. Ф. Принципиальные задачи классификации и анализа моделей для программно-прогностического контроля мультисервисных телекоммуникационных сетей [Текст] / Н. Ф. Казакова, Н. М. Билык, Г. А. Гундериц // Вісник національного університету кораблебудування. — 2010. — № 2(431). — С. 125-132.
161. Скопа, О. О. Аналіз основної дефініції витраткової та прибуткової частини бюджету захищеної інтелектуальної мережі [Текст] / Скопа О.О. // Наукові записки Міжнародного гуманітарного університету. — 2009. — № 16. — С. 112-115.
162. Скопа, О. О. Завадостійкість приймання цифрових сигналів у комп'ютерних радіомережах [Текст] / А. А. Скопа // Гармонізація суспільства – новітній напрямок розвитку держави : Всеукр. наук. конф. аспірантів та молодих вчених, 25 березня 2014 р. : матер. конф. — Одеса, ОНЕУ. — С. 4-6.
163. Вавілов, Є. В. Фактори впливу на показники якості інформаційно-комунікаційних мереж [Текст] / Є. В. Вавілов, Г. В. Васильченко // Гармонізація суспільства – новітній напрямок розвитку держави : Всеукр. наук. конф. аспірантів та молодих вчених, 25 березня 2014 р. : матер. конф. — Одеса, ОНЕУ. — С. 7-10.
164. Петров, А. О. Безпроводне передавання даних в комп'ютерних радіомережах [Текст] / А. О. Петров, Ю. В. Щербина // Гармонізація суспільства – новітній напрямок розвитку держави : Всеукр. наук. конф. аспірантів та молодих вчених, 25 березня 2014 р. : матер. конф. — Одеса, ОНЕУ. — С. 11-14.
165. Аль-Джамалі, А.-М. Сфери застосування інформаційних технологій [Текст] / А.-М. Аль-Джамалі, О. Мацків // Гармонізація суспільства – новітній напрямок розвитку держави : Всеукр. наук. конф. аспірантів та молодих вчених, 25 березня 2014 р. : матер. конф. — Одеса, ОНЕУ. — С. 49-53.
166. Атанасов, М. Вплив інформаційних технологій на розвиток підприємства. [Текст] / М. Атанасов, О. Йона // Гармонізація суспільства – новітній напрямок розвитку держави : Всеукр. наук. конф. аспірантів та

- молодих вчених, 25 березня 2014 р. : матер. конф. — Одеса, ОНЕУ. — С. 54-61.
167. Бандура, О. Інформаційні системи на виробництві [Текст] / О. Бандура, А. Вакула // Гармонізація суспільства – новітній напрямок розвитку держави : Всеукр. наук. конф. аспірантів та молодих вчених, 25 березня 2014 р. : матер. конф. — Одеса, ОНЕУ. — С. 62-66.
168. Янгьоз, О. Інформаційні системи в статистиці [Текст] / О. Янгьоз, О. Єсіна // Гармонізація суспільства – новітній напрямок розвитку держави : Всеукр. наук. конф. аспірантів та молодих вчених, 25 березня 2014 р. : матер. конф. — Одеса, ОНЕУ. — С. 67-72.
169. Баланюк, Ю. Інформаційні системи в державному управлінні [Текст] / Ю. Баланюк, О. Скопа // Гармонізація суспільства – новітній напрямок розвитку держави : Всеукр. наук. конф. аспірантів та молодих вчених, 25 березня 2014 р. : матер. конф. — Одеса, ОНЕУ. — С. 73-79.
170. Осипенко, Д. Інформаційні системи в освіті: питання відкритої освіти і дистанційного навчання [Текст] / Д. Осипенко, С. Ясинська // Гармонізація суспільства – новітній напрямок розвитку держави : Всеукр. наук. конф. аспірантів та молодих вчених, 25 березня 2014 р. : матер. конф. — Одеса, ОНЕУ. — С. 80-84.
171. Петров, А. Інформаційні системи в освіті: технології дистанційного навчання [Текст] / А. Петров, С. Ясинська // Гармонізація суспільства – новітній напрямок розвитку держави : Всеукр. наук. конф. аспірантів та молодих вчених, 25 березня 2014 р. : матер. конф. — Одеса, ОНЕУ. — С. 85-89.
172. Пархуць, Л. Інформаційні системи в освіті: автоматизовані навчальні системи [Текст] / Л. Пархуць, С. Ясинська // Гармонізація суспільства – новітній напрямок розвитку держави : Всеукр. наук. конф. аспірантів та молодих вчених, 25 березня 2014 р. : матер. конф. — Одеса, ОНЕУ. — С. 90-94.
173. Мінін, А. Інформаційні системи в освіті: електронний підручник [Текст] / А. Мінін, С. Ясинська // Гармонізація суспільства – новітній напрямок розвитку держави : Всеукр. наук. конф. аспірантів та молодих вчених, 25 березня 2014 р. : матер. конф. — Одеса, ОНЕУ. — С. 95-101.
174. Современные методы проверки аутентичности магнитных фонограмм в судебно-акустической экспертизе [Текст] / Рыбальский О. В., Жариков Ю. Ф. – К. : НАВСУ, 2003. – 300 с.
175. Застосування вейвлет-аналізу для виявлення слідів цифрової обробки аналогових і цифрових фонограм у судово-акустичній експертизі [Текст] / Рибальський О.В. – К. : НАВСУ, 2004. – 167 с.
176. Рыбальский, О. В. Основные положения теории выявления следов цифровой обработки фонограмм и особенности ее программной и методической реализации в экспертизе материалов и средств видео-

- звукозаписи : ч. 1 [Текст] / О. В. Рыбальский // Захист інформації. – 2006. - № 1. – С. 71–76.
177. Рыбальский О. В. Основные положения теории выявления следов цифровой обработки фонограмм и особенности ее программной и методической реализации в экспертизе материалов и средств видеозвукозаписи : ч 2 [Текст] / О. В. Рыбальский // Захист інформації. – 2006. - № 2. – С. 75–78.
178. Життєвий цикл програмного забезпечення [Електронний ресурс] / Портал : wikipedia. — Режим доступу \www/ URL: http://uk.wikipedia.org/wiki/Життєвий_цикл_програмного_забезпечення. — Заголовок з екрану, доступ вільний, 30.09.2013.
179. Рыбальский, О. В. К вопросу о фрактальности аналоговых сигналов, подвергнутых цифровой обработке [Текст] / О. В. Рыбальский // Вісник Східноукраїнського національного університету ім В. Даля. – 2006. - № 9. - Т. 1. – С. 21–25.
180. Кобозева, А. А. Комплексный подход к экспертизе подлинности материалов цифровой звукозаписи // А. А. Кобозева, О. В. Рыбальский, И. А. Струк, Е. А. Трифонова [Текст] / Вісник Східноукраїнського національного університету ім В. Даля. – 2009. - № 6(136). – С. 75 – 78.
181. Корченко, О. Г. Удосконалення проведення процедури прийняття рішень державних експертів з питань таємниць у сфері оборони засобами інформаційних технологій / Доповіді та тези доповіді міжвідомчої науково-практичної конференції "Сучасні проблеми захисту інформації з обмеженим доступом", Київ, 20-21 лист. 2008 р. // О. Г. Корченко, Ю. О. Дрейс. – К. : НАУ, НА СБУ. – 2008. – С. 62-63.
182. Дрейс, Ю. О. Розрахунок коефіцієнтів захищеності відомостей, що становлять державну таємницю [Текст] / Ю. О. Дрейс, Н. С. Вишневська, Ю. Є. Хохлачова // Захист інформації. - 2010. - № 3(48). - Т. 12. - С. 10-14.
183. Дрейс, Ю. О. Функціонування системи охорони державної таємниці в Україні: організаційно-правова структура, принципи та завдання [Текст] / Ю. О. Дрейс // Безпека інформації. - 2014. - № 2. - Т. 20. - С. 176-184.
184. Оцінювання шкоди національній безпеці України у разі витоку державної таємниці : монографія [Текст] / О. Г. Корченко, О. Є. Архипов, Ю. О. Дрейс. - К. : НА СБ України. - 332 с.
185. Петришин, Л. Б. К определению свойств унитарной системы счисления [Текст] / Л. Б. Петришин, А. А. Борисенко // Електроніка та системи управління. – 2008. – № 3. – С. 17.
186. Петришин, Л. Удосконалення методики складання фінансової звітності підприємства [Текст] / Л. Петришин, Г. Сиротюк // Вісник

- Львівського національного аграрного університету. - 2013. - № 20(1). - С. 178-185.
187. Борщ, В. І. Магістральні пристрої синхронізації другого рівня інформаційних інфраструктур [Текст] / В. І. Борщ, В. В. Коваль // Вісник УН-ДІЗ. – 2006. – №. 1. – С. 64-69.
188. Коваль, В. В. Право на доступ до інформації [Текст] / В. В. Коваль // Проблеми правознавства та правоохоронної діяльності. – 2011. – №. 3. – С. 241-246.
189. Оптимизация структур больших систем : монография [Текст] / Борщ В. И., Донец В. А., Коваль В. В., Лейбзон А. Я., Лесовой Н. П. - К. : Наукова думка, 2000. - 191 с.
190. Терминальное оборудование цифровых сетей электросвязи с интеграцией служб : монография [Текст] / Борщ В. И., Вивчарюк А. В., Донец В. А., Коваль В. В., Лесовой И. П., Орленко Н. П. – К. : Наукова думка, 1999. – 320 с.
191. Борщ, В. И. Выделители тактового синхросигнала цифровых систем передачи и сетей электросвязи [Текст] / В. И. Борщ, В. В. Коваль, Б. Я. Костик, Ю. Г. Туманов // Вісник УБЕНТЗ. - 1999. - № 8. - С. 42-47.
192. Кудинов, В. А. Оптимизация структуры информационной сети [Текст] / В. А. Кудинов, Л. Т. Пархуць, В. А. Хорошко // Захист інформації. – 2004. – №. 3. – С. 44-49.
193. Методы практической криптографии : монография [Текст] / Мухачев В.А., Хорошко В.А. - К. : ООО Полиграф-Консалтинг. – 2005. – 215 с.
194. Казакова, Н. Ф. Організація процесу розробки програмного забезпечення для захищених інформаційних систем [Текст] / Н. Ф. Казакова // Сучасний захист інформації. — К. : ДУІКТ. — 2010. — №2. — С. 48-56.
195. Хорошко, В. А. Модель системы защиты информации [Текст] / В. А. Хорошко // Захист інформації. – 1999. – №. 1. – С. 5-11.
196. Хорошко, В. А. Модель системы защиты информации [Текст] / В. А. Хорошко // Захист інформації. – 1999. – №. 1. – С. 5-11.
197. Kanade, T. The image stabilizer plugin for Image [Електронний ресурс] / Т. Kanade, В. Lucas // Портал : без назви. — Режим доступу \www/ URL: http://www.cs.cmu.edu/~kangli/code/Image_Stabilizer.html. — Заголовок з екрану, доступ вільний, 30.10.2012.
198. Прэтт, У. Цифровая обработка изображений [Текст] : пер. с англ. / У. Прэтт. — В 2-х кн. — М. : Мир, 1982. — 792 с.
199. Kaas, M. Analyzing oriented patterns [Текст] / М. Kaas, А. Witkin // Comput. Vision Graphics Image Process. — 1987. — 362-385.
200. Terzopoulos, D. Regularization of inverse visual problems involving discontinuities [Текст] / D. Terzopoulos // IEEE Trans. PAMI. — 1986. — №4(8). — pp. 413-424.

201. Arulampalam, M. A Tutorial on Particle Filters for Online Nonlinear/ Non-Gaussian Bayesian Tracking [Текст] / M. Arulampalam, S. Maskell, N. Gordon, T. Clapp // IEEE Transactions on Signal Processing. — 2002. — Vol. 50. — №2. — pp. 174-188.
202. Gonzalez, R. Digital Image Processing [Електронний ресурс] / R. Gonzalez, R. Woods // Addison Wesley Longman. — AWL, Inc. — 1992. — Портал : без назви. — Режим доступу \www/ URL: 202.197.67.17/yxtxcl/xtysj/dip_answer.pdf. — Заголовок з контейнера, доступ вільний, 30.10.2012.
203. Wilamowski, B. M. Computing Gradient Vector and Jacobian Matrix in Arbitrarily Connected Neural Networks [Текст] / B. M. Wilamowski та ін. — IEEE Transactions On Industrial Electronics. — 2008. — Т. 55. — №10. — С. 3784-3790.
204. Математические методы распознавания образов [Електронний ресурс] : Доклады XI Всерос. конф. (окт. 2003) / отв. ред. Ю. И. Журавлев. — М. : РАН, 2003. — 511 с. — Портал : без назви. — Режим доступу \www/ URL: http://window.edu.ru/resource/825/50825/files/mmro11.pdf. — Заголовок з контейнера, доступ вільний, 30.10.2012.
205. Polygonal Modeling [Електронний ресурс] / Портал : без назви. — Режим доступу \www/ URL: http://www.arch.cuhk.edu.hk/server1/staff1/marcaurel/desc9019/tutorials/Readings/mayaDocs/PolygonalModeling.pdf. — Заголовок з контейнера, доступ вільний, 28.09.2012.
206. Spline [Електронний ресурс] / Портал : En.wikipedia. — Режим доступу \www/ URL: http://en.wikipedia.org/wiki/Spline_(mathematics). — Заголовок з екрану, доступ вільний, 23.10.2012.
207. Оператор Собеля [Електронний ресурс] / Портал : Ru.wikipedia. — Режим доступу \www/ URL: http://ru.wikipedia.org/wiki/оператор_Собеля. — Заголовок з екрану, доступ вільний, 16.10.2012.
208. Prescott New Instructions (SSE3): обзор новых SIMD расширений с точки зрения разработки и оптимизации программного обеспечения [Електронний ресурс] / Портал : ixbt. — Режим доступу \www/ URL: http://www.ixbt.com/cpu/sse3.shtml. — Заголовок з екрану, доступ вільний, 17.10.2012.
209. Методи згладжування та корекції зображень [Електронний ресурс] / Портал : без назви. — Режим доступу \www/ URL: http://www.kazedu.kz/referat/192238. — Заголовок з екрану, доступ умовно-вільний, 17.10.2012.
210. Оператор Лапласа [Електронний ресурс] / Портал : Wikipedia. — Режим доступу \www/ URL: http://ru.wikipedia.org/wiki/оператор_Лапласа. — Заголовок з екрану, доступ вільний, 05.11.2012.

211. Оператор Набла в различных системах координат [Электронный ресурс] / Портал : Ru.wikipedia. — Режим доступа \www/ URL: http://ru.wikipedia.org/wiki/Оператор_Набла_в_различных_системах_к_оординат. — Заголовок з екрану, доступ вільний, 05.11.2012.
212. Формула Тейлора. Степенные ряды [Электронный ресурс] / Портал : Прикладная математика. — Режим доступа \www/ URL: <http://www.rm298.ru/tei.php>. — Заголовок з екрану, доступ вільний, 05.11.2012.
213. Тиман, А. Ф. Введение в теорию гармонических функций : монография / А. Ф. Тиман, В. Н. Трофимов. — М. : Наука, 1968. — 208 с.
214. Коэффициенты Ламе [Электронный ресурс] / Портал : Wikia. — Режим доступа \www/ URL: http://ru.math.wikia.com/wiki/Коэффициенты_Ламе. — Заголовок з екрану, доступ вільний, 04.11.2012.
215. Риманова метрика [Электронный ресурс] / Портал : Академик. — Режим доступа \www/ URL: http://dic.academic.ru/dic.nsf/enc_mathematics/4844/Риманова. — Заголовок з екрану, доступ вільний, 30.09.2012.
216. Laplace-Beltrami operator [Электронный ресурс] / Портал : en.wikipedia. — Режим доступа \www/ URL: http://en.wikipedia.org/wiki/Laplace-Beltrami_operator. — Заголовок з екрану, доступ вільний, 30.09.2012.
217. Дискретный оператор Лапласа [Электронный ресурс] / Портал : wikipedia. — Режим доступа \www/ URL: http://ru.wikipedia.org/wiki/Дискретный_оператор_Лапласа. — Заголовок з екрану, доступ вільний, 27.09.2012.
218. Модель Ізінга [Электронный ресурс] / Портал : uk.wikipedia. — Режим доступа \www/ URL: http://uk.wikipedia.org/wiki/Модель_Ізінга. — Заголовок з екрану, доступ вільний, 05.11.2012.
219. Петльова квантова гравітація [Электронный ресурс] / Портал : uk.wikipedia. — Режим доступа \www/ URL: http://uk.wikipedia.org/wiki/Петльова_квантова_гравітація. — Заголовок з екрану, доступ вільний, 27.09.2012.
220. Динамічна система [Электронный ресурс] / Портал : uk.wikipedia. — Режим доступа \www/ URL: http://uk.wikipedia.org/wiki/Динамічна_система. — Заголовок з екрану, доступ вільний, 28.09.2012.
221. Способы задания графов и операции над графами [Электронный ресурс] / Портал : Образовательный блог — всё для учебы. — Режим доступа \www/ URL: <http://all4study.ru/matematika/sposoby-zadaniya-grafov-i-operacii-nad-grafami.html>. — Заголовок з екрану, доступ вільний, 09.09.2012.
222. Усредняющий оператор [Электронный ресурс] / Портал : Академик. — Режим доступа \www/ URL: http://universal_ru_en.academic.ru/2891741/Усредняющий_оператор. — Заголовок з екрану, доступ вільний, 21.09.2012.

223. Собственные векторы, значения и пространства [Электронный ресурс] / Портал : ru.wikipedia. — Режим доступа \www/ URL: http://ru.wikipedia.org/wiki/Собственные_векторы,_значения_и_пространства, 05.11.2012.
224. Шрёдингера оператора спектр [Электронный ресурс] / Портал : Академик. — Режим доступа \www/ URL: http://dic.academic.ru/dic.nsf/enc_physics/5233/Шрёдингера. — Заголовок з екрану, доступ вільний, 27.09.2012.
225. Гамильтониан [Электронный ресурс] / Портал : Энциклопедия физики и техники. — Режим доступа \www/ URL: http://www.femto.com.ua/articles/part_1/0668.html. — Заголовок з екрану, доступ вільний, 28.09.2012.
226. Теорема Стоуна про представления булевых алгебр [Электронный ресурс] / Портал : uk.wikipedia. — Режим доступа \www/ URL: http://uk.wikipedia.org/wiki/Теорема_Стоуна_про_представления_булевых_алгебр. — Заголовок з екрану, доступ вільний, 01.10.2012.
227. Функция Грина [Электронный ресурс] / Портал : Wikia. — Режим доступа \www/ URL: http://ru.math.wikia.com/wiki/Функция_Грина. — Заголовок з екрану, доступ вільний, 01.10.2012.
228. Резольвента [Электронный ресурс] / Портал : без назви. — Режим доступа \www/ URL: <http://znaimo.com.ua/Резольвента.doc>. — Заголовок з контейнера, доступ вільний, 01.10.2012.
229. Символ Кронекера [Электронный ресурс] / Портал : Викизнание. — Режим доступа \www/ URL: http://www.wikiznanie.ru/ru-wz/index.php/Символ_Кронекера. — Заголовок з екрану, доступ вільний, 01.10.2012.
230. База данных [Электронный ресурс] / Портал : Википедия — свободная энциклопедия. — Режим доступа \www/ URL: http://www.ru.wikipedia.org/wiki/База_данных. — Заголовок з екрану, доступ вільний, 30.10.2012.
231. Авторское право [Электронный ресурс] / Портал : Википедия — свободная энциклопедия. — Режим доступа \www/ URL: http://www.ru.wikipedia.org/wiki/Авторское_право. — Заголовок з екрану, доступ вільний, 30.10.2012.
232. Закон України «Про авторське право і суміжні права» від 23 грудня 1993 року [Электронный ресурс] / Портал : Верховна Рада України. — Режим доступа \www/ URL: <http://www.zakon2.rada.gov.ua/laws/show/3792-12>. — Заголовок з екрану, доступ вільний, 31.10.2012.
233. Толпеев, А.С. Проблема защиты авторского права на базы данных [Электронный ресурс] / Портал : Международная полицейская корпорация гражданской безопасности. — Режим доступа \www/ URL: <http://www.mprkgb-mykolaiv.at.ua/publ/1-1-0-1>. — Заголовок з екрану, доступ вільний, 31.10.2012.

234. Залесов, А. В. Защита авторских прав на базу данных — новое оружие в конкурентной борьбе? [Текст] / А. В. Залесов // Биржа интеллектуальной собственности. — М. : Международный институт промышленной собственности. — 2006. — №3 / Портал : Sojuzpatent. — Режим доступа \www/ URL: <http://www.sojuzpatent.com/doc/ПравОхрБД.doc>. — Заголовок з екрану, доступ вільний, 09.09.2010.
235. Відновлення та оптимізація інформації в системах прийняття рішень : підручник [Текст] / В. Л. Баранов, М. М. Браїловський, А. А. Засядько, Н. Ф. Казакова, В. О. Хорошко. — К. : ДУІКТ, 2009. — 134 с..
236. Фразе-Фразенко О.О. Использование биометрических термопоказателей для идентификации в системах доступа // Східно-Європейський журнал передових технологій. — №1/1(9) 2013. — Харків. — С.33-35
237. Рыбальский О. В. Застосування вейвлет-аналізу для виявлення слідів цифрової обробки аналогових і цифрових фонограм у судово-акустичній експертизі : монографія. — К. : НАВСУ, 2004. — 167 с.
238. Рыбальский О. В., Жариков Ю. Ф. Современные методы проверки аутентичности магнитных фонограмм в судебно-акустической экспертизе : монография. — К. : НАВСУ, 2003. — 300 с.
239. Рыбальский, О. В. Анализ возможных цифровых и аналоговых способов подделки фонограмм и требований к анализаторам для выявления их следов [Текст] / О. В. Рыбальский // Захист інформації. — 2004. — Спеціальний випуск. — С. 44-48.
240. Рыбальский, О. В. К вопросу о фрактальности аналоговых сигналов, подвергнутых цифровой обработке [Текст] / О. В. Рыбальский // Вісник Східноукраїнського національного університету імені Володимира Даля. — 2006. — № 9. — Ч. 1. — С. 21-25.
241. Рыбальский, О. В. Некоторые проблемы современной фоноскопической экспертизы [Текст] / О. В. Рыбальский // Спеціальна техніка у правоохоронній діяльності : IV міжнар. наук.-практ. конф., 26-27 листопада 2009 р. : матер. конф. — Київ, КНУВС. — 3 с.
242. Рыбальский, О. В. Основные положения теории выявления следов цифровой обработки фонограмм и особенности ее программной и методической реализации в экспертизе материалов и средств видеозвукозаписи. Часть 1 [Текст] / О. В. Рыбальский // Захист інформації. — 2006. — № 1. — С. 71-76.
243. Рыбальский, О. В. Программа идентификации цифровой фото- и видеоаппаратуры и проверки оригинальности цифровых изображений [Текст] / О. В. Рыбальский, В. И.Соловьев, Е. В. Белозеров // Вісник Київського національного університету ім. Т. Шевченко. Військово-спеціальні науки. — 2013. — Спеціальний випуск. — С. 77-80.
244. Скопа, О. О. Анізотропна фільтрація зображень у системах аутентифікації [Текст] / О. О. Скопа, О. О. Фразе-Фразенко // Захист

інформації і безпека інформаційних систем : II міжнар. наук.-техн. конф., 30 травня — 01 червня 2013 р. — НУ «Львівська політехніка», Львів. — С. 156-158.

245. Соловьев, В. И. Система идентификации аппаратуры аудиозаписи на основе мультифрактального подхода [Текст] / В. И. Соловьев, О. В. Рыбальский // Вісник Східноукраїнського національного університету імені Володимира Даля. — 2010. — № 9(151). — Ч. 1. — С. 58-63.
246. Фразе-Фразенко О. О. Исследование и применение в системах защиты информации корреляционного критерия сходства графических структур : монография // Информационные системы в управлении, образовании, промышленности [Текст] / Н. Ф. Казакова, О. О. Фразе-Фразенко [и др.] ; под ред. В. С. Пономаренко. — Х. : ТОВ «Щедра садиба плюс», 2014. — 498 с.
247. Фразе-Фразенко О.О. Алгоритм навчання нейронної мережі при розпізнаванні зображень // Східно-Європейський журнал передових технологій. — №4/1(6) 2012. — Харків. — С.33-34.
248. Фразе-Фразенко, О. О. Спосіб регуляризації некоректно поставленої задачі розпізнавання у системах телебачення замкнутого контуру [Текст] / О. О. Фразе-Фразенко // Східно-Європейський журнал передових технологій. — 2012. — № 6/4(8). — С. 19-20. — ISSN 1729-3774.
249. Скопа, О. О. Роль телекомунікацій в сучасному бізнесі [Текст] / О. О. Скопа, Н. Ф. Казакова // Наукові праці УДАЗ: Період. наук. збір. з радіотехніки і телекомунікацій, електроніки та економіки в галузі зв'язку. — Одеса : УДАЗ. — 1999. — № 2. — С. 11-12.
250. Казакова, Н. Ф. Надійність функціонування морських супутникових систем телекомунікацій [Текст] / Н. Ф. Казакова // Збірник наукових праць Українського державного морського технічного університету. — Миколаїв : УДМТУ. — 2002. — № 7(385). — С. 109-115.
251. Казакова, Н. Ф. Принципи побудови систем управління радіозв'язком з рухомими об'єктами [Текст] / Н. Ф. Казакова // Вісник Національного університету «Львівська політехніка»: Збірн. наук. праць. — Львів : НУ «Львівська політехніка». — 2002. — № 443. — С. 86-89.
252. Казакова, Н. Ф. Рекуррентный полиномиальный метод линейного программирования [Текст] / Н. Ф. Казакова // Наукові праці ДонДТУ. Серія: Обчислювальна техніка та автоматизація. — Донецьк : РВА ДонДТУ. — 2002. — № 47. — С. 240-248.
253. Корчинський, В. В. Аналіз статистики помилок в системах передачі даних зі змінними параметрами [Текст] / В. В. Корчинський, Н. Ф. Казакова, Н. А. Тринтіна // Наукові праці ОНАЗ : період. наук. збір. з радіотехніки і телекомунікацій, електроніки та економіки в галузі зв'язку. — Одеса : ОНАЗ. — 2002. — №1. — С. 85-94.
254. Казакова, Н. Ф. Аналітичне розв'язання одновимірної задачі Клопера-Пірсона [Текст] / Н. Ф. Казакова // Радиотехника: Всеукр. межве-

- домств. научн.-техн. сб. — Харьков : ХНУРЭ. — 2002. — № 128. — С. 97-98.
255. Скопа, А. А. Применение теории псевдополубратных матриц к решению задач по оценке надежности систем телекоммуникаций. Часть 1. Общие положения [Текст] / А. А. Скопа, Н. Ф. Казакова // Праці УНДІРТ. — Одеса : УНДІРТ. — 2002. — № 4(32). — С. 88-91.
256. Казакова, Н. Ф. Установление критериев оптимизации алгоритмов при определении эффективности информационных систем [Текст] / Н. Ф. Казакова, И. О. Годулян, О. О. Чуприна // Наукові записки УНДІЗ. — К. : УНДІЗ. — 2007. — № 1. — С. 62-71.
257. Казакова, Н. Ф. Скорочення обсягів контрольних випробувань в інформаційних системах за рахунок їх функціональної надмірності [Текст] / Н. Ф. Казакова, Н. М. Согіна // Моделювання та інформаційні технології: зб. наук. праць ІПМЕ НАН України. — К. : ІПМЕ НАН України. — 2008. — № 49. — С. 34-40.
258. Скопа, О. О. Проектний аналіз оцінювання ступеня ризику при скороченні обсягу профілактичних вимірювань об'єктів інфомереж [Текст] / О. О. Скопа, Н. Ф. Казакова // Вісник Львівського національного аграрного університету: Агроінженерні дослідження. — Львів : Львівськ. нац. агроуніверситет. — 2008. — № 12. — Т. 1. — С. 66-71.
259. Хорошко, В. О. Наукові задачі синтезу організаційно-технологічної схеми створення програмного забезпечення для комп'ютерних мереж з обмеженим доступом [Текст] / В. О. Хорошко, Н. Ф. Казакова // Захист інформації. — К. : НАУ. — 2009. — № 4(45). — С.11-18. — Індексация у МНМБ: НЭБ Library.ru, Simple Search Metadata, OCLC WorldCat, Base, ULRICHS WEB.
260. Хорошко, В. А. Выделение оптимальной совокупности подпрограмм из основной программы работы системы защиты информации [Текст] / В. А. Хорошко, Н. Ф. Казакова, Г. А. Сирченко, Е. О. Тискина // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. — Київ : ВІ КНУ імені Тараса Шевченка. — 2010. — № 26. — С. 138-142.
261. Скопа, О. О. Встановлення ступеню ризику підприємства при скороченні обсягу профілактичних вимірювань [Текст] / О. О. Скопа, Н. Ф. Казакова, Є. О. Мініна // Вісник Східноукраїнського національного університету імені Володимира Даля. — Луганськ : СНУ ім. В. Даля. — 2011. — № 7(161). — Т. 1. — С. 138-141.
262. Скопа, А. А. Политика предупреждения угроз информационной безопасности в практической деятельности Одесского филиала ОАО «Укртелеком» [Текст] / А. А. Скопа, Н. Ф. Казакова, С. Т. Сорока // Вісник Національного технічного університету «ХПІ» : Нові рішення в сучасних технологіях. — Х. : НТУ «ХПІ». — 2012. — № 17. — С. 42-47.
263. Казакова, Н. Ф. Оцінка живучості систем моніторингу інформаційного простору [Текст] / Н. Ф. Казакова // Восточно-европейский журнал передовых технологий. — Харьков : Технологический центр. — 2012. —

- № 4/2(58). — С. 12-15. — Індексція у МНМБ: НЭБ Library.ru, OCLC WorldCat, BASE, ULRICHS WEB, Driver, Index Copernicus, DOAJ, EBSCO publishing, ResearchBIB
264. Казакова, Н. Ф. Некоректні задачі відновлення даних у системах моніторингу інформаційного простору [Текст] / Н. Ф. Казакова // Вісник Східноукраїнського національного університету імені Володимира Даля. — Луганськ : СЧУ ім. В.Даля. — 2012. — № 8(179). — Т. 1. — С. 325-332.
265. Волков, С. Л. Оптимізація параметрів телекомунікаційної мережі методом статистичної регуляризації [Текст] / С. Л. Волков, Н. Ф. Казакова // Сучасна спеціальна техніка. — К. : Державний науководослідний інститут МВС України. — 2012. — № 1(28). — С. 54-60.
266. Казакова, Н. Ф. Застосування програмно реалізованого прогностичного контролю для вирішення практичних завдань забезпечення якості надання послуг у захищених інформаційних мережах [Текст] / Н. Ф. Казакова // Сучасна спеціальна техніка. — К. : Державний науководослідний інститут МВС України. — 2012. — № 2(29). — С. 86-95.
267. Петров А. О. Моделі розв'язання задачі про відновлення інформації [Текст] / А. О. Петров, Н. Ф. Казакова // Збірник наукових праць Київського національного університету імені Тараса Шевченка. — К. : ВІКНУ. — 2012. — № 38. — С. 186-192.
268. Казакова, Н. Ф. Теореми до теорії випробування надійності автоматичних систем однократного використання [Текст] / Н. Ф. Казакова, А. В. Мінін // Інформаційна безпека. — Луганськ : СЧУ ім. В.Даля. — 2012. — № 2(8). — С. 60-72. — ISSN 2224-9613.
269. Казакова, Н. Ф. Проблеми правового забезпечення захисту баз даних [Текст] / Н. Ф. Казакова, Ю. В. Щербина // Інформаційна безпека. — Луганськ : СЧУ ім. В.Даля. — 2012. — № 2(8). — С. 73-76. — ISSN 2224-9613.
270. Казакова, Н. Ф. Управління життєвим циклом програмних засобів [Текст] / Н. Ф. Казакова // Восточно-европейский журнал передовых технологий. — Харьков : Технологический центр. — 2013. — № 3/10(63). — С. 8-12. — Індексція у МНМБ: НЭБ Library.ru, OCLC WorldCat, BASE, ULRICHS WEB, Driver, Index Copernicus, DOAJ, EBSCO publishing, ResearchBIB
271. Казакова, Н. Ф. Проблема моделювання трафіку у мережах доступу до недовірених систем [Текст] / О. А. Сиропятов, Н. Ф. Казакова // Інформаційна безпека. — Луганськ : СЧУ ім. В. Даля. — 2013. — № 1(9). — С.185-189. — ISSN 2224-9613.
272. Йона, О. О. Світові тенденції боротьби з кіберзлочинністю [Текст] / О. О. Йона, Н. Ф. Казакова // Вісник Східноукраїнського національного університету імені Володимира Даля. — Луганськ : СЧУ ім. В. Даля. — 2013. — № 15(204). — Т. 1. — С. 59-62.

273. Казакова, Н. Ф. Міжнародна регламентація правового регулювання та стандартизації аудиту інформаційної безпеки [Текст] / Н. Ф. Казакова, Е. А. Плешко, К. Б. Айвазова // Вісник Східноукраїнського національного університету імені Володимира Даля. — Луганськ : СНУ ім. В.Далія. — 2013. — № 15(204). — Т. 1. — С. 172-181.
274. Казакова, Н. Ф. Автоматизація процесу адаптації інформаційних систем до інцидентів інформаційної безпеки [Текст] / Н. Ф. Казакова, Є. В. Вавілов // Інформаційна безпека. — Луганськ : СНУ ім. В. Далія. — 2013. — №4(12). — С. 49-56. — ISSN 2224-9613.
275. Kazakova, Nadia. Model that Solve the Information Recovery Problems [Текст] / Nadia Kazakova, Oleksandr Skopa, Mikołaj Karpiński // Journal of Telecommunications and Information Technology. — 2014. — №4. — P. 1-5.
276. Казакова, Н. Ф. Розробка нового еволюційного рівня моделі обслуговування IaaS/PaaS/SaaS [Текст] / Н. Ф. Казакова, О. В. Грабовський // Восточно-европейский журнал передовых технологий. — 2014. — № 5/2(71). — С. 38-41.
277. Мухін, О. М. Планування обсягу випробувань в мережах телекомунікацій [Текст] / О. М. Мухін, Н. Ф. Казакова, О. О. Скопа // Вісник УБЕНТЗ. — К. : УБЕНТЗ. — 2002. — № 2. — С. 104-109.
278. Казакова, Н. Ф. Технічне рішення задачі Клопера-Пірсона [Текст] / Н. Ф. Казакова // Наукові записки Міжнародного гуманітарного університету. — Одеса : МГУ. — 2005. — № 3. — С. 89-94.
279. Чепок, А. О. Международная значимость Европейского научного пространства в 1-й декаде XXI века [Текст] / А. О. Чепок, Н. Ф. Казакова // Наукові записки Міжнародного гуманітарного університету. — Одеса : МГУ. — 2008. — № 13. — С. 24-44.
280. Рубежанський, Ю. С. Использование политики предупреждения инцидентов в практической деятельности Центра обработки данных Одесского филиала ОАО «Укртелеком» [Текст] / Ю. С. Рубежанський, С. Т. Сорока, Н. Ф. Казакова // Наукові записки Міжнародного гуманітарного університету. — Одеса : МГУ. — 2009. — № 16. — С. 122-127.
281. Казакова, Н. Ф. Модель та структурно-функціональний склад терміналу радіодоступу при дослідженнях систем захисту інформації в Cross-П РС ДСВМ в умовах радіоелектронної протидії [Текст] / Н. Ф. Казакова, О. В. Грабовський // Проблеми технічного регулювання та якості : IV Всеукр. наук.-практ. конф., 9-10 жовтня 2014 р. ¼ ОДАТРЯ, Одеса. ¾ С. 109-112.
282. Казакова Н., Йона О. Тенденції захисту від кіберзлочинів // Матеріали III Міжнар. наук.-техн. конф. «Захист інформації і безпека інформаційних систем», 5-6 червня 2014 року, НУ «Львівська політехніка. м. Львів. — С. 20-21.

283. Волков С.Л., Казакова Н.Ф. Анализ качества предоставления услуг Интернет-провайдерами // 36. наук. праць II наук.-практ. конф. «Інформаційно-вимірвальні технології, технічне регулювання», Одеса, 17 листопада 2011 р. — Одеса: Одеська державна академія технічного регулювання та якості, 2011. — С. 84-89.
284. Казакова Н., Щербина Ю., Соловйов О. Забезпечення порівнянності результатів оцінки захищеності автоматизованих систем // Матеріали II-ої Міжнар. наук.-техн. конф. «Захист інформації і безпека інформаційних систем», Львів, 30 травня — 01 червня 2013 р. — Львів : НУ «Львівська політехніка», 2013. — С. 158-160.
285. Казакова Н.Ф., Петров А.О. Питання теорії детермінованої регуляризації некоректних задач відновлення інформації в системах моніторингу спеціального призначення // Матеріали III-ї Всеукр. наук.-практ. конф. «Інформаційно-вимірвальні технології в метрології, технічне регулювання та менеджмент якості», Одеса, 30-31 травня 2013 р. — Одеса : Одеська державна академія технічного регулювання та якості, 2013. — С. 81-83.
286. Скопа О., Казакова Н. Проектний аналіз оцінювання ступеня ризику при скороченні обсягу профілактичних вимірювань об'єктів інфомереж // Матеріали IX Міжнар. наук.-практ. конф. «Сучасні проблеми землеробської механіки» присвяченій 108-й річниці з дня народження академіка П.Василенка, Львів-Дубляни, 17-18 жовтня 2008 року. — Львів: Львівський національний аграрний університет. — С.17.
287. Скопа А.А., Хорошко В.А., Казакова Н.Ф. Развитие технологии программного моделирования защищенной транспортной сети // Матеріали I Міжнар. наук.-практ. конф. «Проблеми й перспективи розвитку ІТ-індустрії», Харків, 18-19 листопада 2009 р. — Харків: Харківський національний економічний ун-т, 2009. — С.196-198.
288. Казакова Н.Ф., Кушер А.Н. Проблемы разработки и анализа теоретических подходов к моделированию трафика защищенных информационных сетей с точки зрения их соответствия сетям нового поколения // Вісник УНДІЗ: Матеріали XI Міжнар. наук.-практ. конф. «Новітні мережні технології в Україні», Партеніт, 28-30 вересня 2009 р. — К.: УНДІЗ. — №3. —2009. — С.84-89.
289. Казакова Н.Ф., Сорока С.Т. Алгоритм действий дежурного персонала при сбоях и событиях в системе информационной безопасности Одесского филиала ОАО «Укртелеком» // Вісник УНДІЗ: Матеріали VIII Міжнар. наук.-практ. конф. «Проблеми управління телекомунікаційними мережами та послугами в умовах конкурентного ринку», Партеніт, 23-25 вересня 2009 р. — К.: УНДІЗ. — №2. — 2009. — С.14-15.
290. Кушер А.М., Казакова Н.Ф. Метод системного багаторівневого прогнозування // Матеріали II Міжнар. наук.-практ. конф. «Обробка сигналів і негаусівських процесів», 25-29 травня 2009 г. — Черкаси: ЧДТУ, 2009.

291. Казакова Н.Ф., Тимофеев Б.В. Аналіз захищеності інформаційних мереж // Комп'ютерні технології, інформаційна безпека та дизайн: Матеріали IV наук.-практ. конф. проф.-викл. складу та студентства Міжнародного гуманітарного ун-ту (секції 7...13), 22 травня 2009 р. — Одеса: МГУ, 2009. — С.71-73.
292. Казакова Н.Ф. Исследование алгоритмов повышения верности в сетях передачи данных с обратной связью // Матер. II звітної наук.-практ. конф. проф.-викл. складу та студентства Міжнар. гуманіт. ун-ту, 12 квітня 2007 р., Одеса: Міжнар. гуманіт. ун-т, 2007. — С.33-35.
293. Фразе-Фразенко О.О. Багатоагентний метод виділення інформативних ознак зображень у системах доступу // Вісник Східноукраїнського національного університету ім. В.Даля — 2013. — №15(204). — Луганськ: СНУ ім. В.Даля. — С.210-218.
294. Фразе-Фразенко О.О. Узагальнення кореляційних властивостей контурів // Інформаційна безпека — 2012. — №2(8). — Луганськ: СНУ ім. В.Даля. — С.158-167.
295. Фразе-Фразенко О.О. Аналіз сплайн-методів з метою їх застосування для обробки контурів зображень // Вісник НТУ «ХПІ» — 2012. — №66(972). — Харків: НТУ «ХПІ». — С.52-63
296. Фразе-Фразенко О.О. Компенсація крайових шумових спотворень на цифровому зображенні // Вісник НТУ «ХПІ» — 2012. — №68(974). — Харків: НТУ «ХПІ». — С.130-135.
297. Фразе-Фразенко, О.О. Метод анізотропної фільтрації нестабільних зображень у системах доступу з біометричною аутентифікацією / Фразе-Фразенко О. О. // Інформаційна безпека. — Луганськ : СНУ ім. В.Даля. — 2013. — №4(12). — С. 112-125. — ISSN 2224-9613.
298. Рибальський, О. В. Практична реалізація технології ідентифікації та оригінальності технічних засобів фіксації цифрових зображень [Текст] / О. В. Рибальський, О. О. Фразе-Фразенко // Проблеми технічного регулювання та якості : IV Всеукр. наук.-практ. конф., 9-10 жовтня 2014 р. — ОДАТРЯ, Одеса. — С. 130-133.
299. Фразе-Фразенко, О. О. Дослідження та застосування у системах ідентифікації кореляційного критерію подібності графічних зображень [Текст] / О. О. Фразе-Фразенко, С. Д. Асабашвілі // Проблеми технічного регулювання та якості : IV Всеукр. наук.-практ. конф., 9-10 жовтня 2014 р. — ОДАТРЯ, Одеса. — С. 113-116.
300. Орлик, О. В. Соціально-економічна концепція інтелектуальної мережі [Текст] / О. В. Орлик, А. Ю. Вакула, Б. Ч. Бердієв // Проблеми технічного регулювання та якості : IV Всеукр. наук.-практ. конф., 9-10 жовтня 2014 р. — ОДАТРЯ, Одеса. — С. 48-51.
301. Скопа, О. О. Завадостійкість приймання цифрових сигналів у комп'ютерних радіомережах [Текст] / А. А. Скопа // Гармонізація суспільства — новітній напрямок розвитку держави : Всеукр. наук. конф.

- аспірантів та молодих вчених, 25 березня 2014 р. : матер. конф. — Одеса, ОНЕУ. — С. 4-6.
302. Вавілов, Є. В. Фактори впливу на показники якості інформаційно-комунікаційних мереж [Текст] / Є. В. Вавілов, Г. В. Васильченко // Гармонізація суспільства — новітній напрямок розвитку держави : Всеукр. наук. конф. аспірантів та молодих вчених, 25 березня 2014 р. : матер. конф. — Одеса, ОНЕУ. — С. 7-10.
303. Петров, А. О. Безпроводне передавання даних в комп'ютерних радіо-мережах [Текст] / А. О. Петров, Ю. В. Щербина // Гармонізація суспільства — новітній напрямок розвитку держави : Всеукр. наук. конф. аспірантів та молодих вчених, 25 березня 2014 р. : матер. конф. — Одеса, ОНЕУ. — С. 11-14.
304. Ясинська, С. Ю. Концепція інформаційно-освітнього середовища: сучасний стан досліджень і розробок в області побудови інформаційно-освітніх середовищ [Текст] / С. Ю. Ясинська, Н. Ф. Казакова // Гармонізація суспільства — новітній напрямок розвитку держави : Всеукр. наук. конф. аспірантів та молодих вчених, 25 березня 2014 р. : матер. конф. — Одеса, ОНЕУ. — С. 15-21.
305. Ясинська, С. Ю. Концепція інформаційно-освітнього середовища: підхід до розробки структури [Текст] / С. Ю. Ясинська, А. Ю. Вакула // Гармонізація суспільства — новітній напрямок розвитку держави : Всеукр. наук. конф. аспірантів та молодих вчених, 25 березня 2014 р. : матер. конф. — Одеса, ОНЕУ. — С. 22-29.
306. Ясинська, С. Ю. Концепція інформаційно-освітнього середовища: дисциплінарне ядро та інформаційно-довідкова база [Текст] / С. Ю. Ясинська, О. Г. Єсіна // Гармонізація суспільства — новітній напрямок розвитку держави : Всеукр. наук. конф. аспірантів та молодих вчених, 25 березня 2014 р. : матер. конф. — Одеса, ОНЕУ. — С. 30-35.
307. Ясинська, С. Ю. Концепція інформаційно-освітнього середовища: застосування наукоємного програмного забезпечення [Текст] / С. Ю. Ясинська, О. О. Фразе-Фразенко // Гармонізація суспільства — новітній напрямок розвитку держави : Всеукр. наук. конф. аспірантів та молодих вчених, 25 березня 2014 р. : матер. конф. — Одеса, ОНЕУ. — С. 36-42.
308. Ясинська, С. Ю. Концепція інформаційно-освітнього середовища: дидактика застосування [Текст] / С. Ю. Ясинська, Г. В. Васильченко // Гармонізація суспільства — новітній напрямок розвитку держави : Всеукр. наук. конф. аспірантів та молодих вчених, 25 березня 2014 р. : матер. конф. — Одеса, ОНЕУ. — С. 43-48.
309. Аль-Джамалі, А.-М. Сфери застосування інформаційних технологій [Текст] / А.-М. Аль-Джамалі, О. Мацків // Гармонізація суспільства — новітній напрямок розвитку держави : Всеукр. наук. конф. аспірантів та молодих вчених, 25 березня 2014 р. : матер. конф. — Одеса, ОНЕУ. — С. 49-53.

310. Атанасов, М. Вплив інформаційних технологій на розвиток підприємства. [Текст] / М. Атанасов, О. Йона // Гармонізація суспільства — новітній напрямок розвитку держави : Всеукр. наук. конф. аспірантів та молодих вчених, 25 березня 2014 р. : матер. конф. — Одеса, ОНЕУ. — С. 54-61.
311. Бандура, О. Інформаційні системи на виробництві [Текст] / О. Бандура, А. Вакула // Гармонізація суспільства — новітній напрямок розвитку держави : Всеукр. наук. конф. аспірантів та молодих вчених, 25 березня 2014 р. : матер. конф. — Одеса, ОНЕУ. — С. 62-66.
312. Янгьоз, О. Інформаційні системи в статистиці [Текст] / О. Янгьоз, О. Єсіна // Гармонізація суспільства — новітній напрямок розвитку держави : Всеукр. наук. конф. аспірантів та молодих вчених, 25 березня 2014 р. : матер. конф. — Одеса, ОНЕУ. — С. 67-72.
313. Баланюк, Ю. Інформаційні системи в державному управлінні [Текст] / Ю. Баланюк, О. Скопа // Гармонізація суспільства — новітній напрямок розвитку держави : Всеукр. наук. конф. аспірантів та молодих вчених, 25 березня 2014 р. : матер. конф. — Одеса, ОНЕУ. — С. 73-79.
314. Осипенко, Д. Інформаційні системи в освіті: питання відкритої освіти і дистанційного навчання [Текст] / Д. Осипенко, С. Ясинська // Гармонізація суспільства — новітній напрямок розвитку держави : Всеукр. наук. конф. аспірантів та молодих вчених, 25 березня 2014 р. : матер. конф. — Одеса, ОНЕУ. — С. 80-84.
315. Петров, А. Інформаційні системи в освіті: технології дистанційного навчання [Текст] / А. Петров, С. Ясинська // Гармонізація суспільства — новітній напрямок розвитку держави : Всеукр. наук. конф. аспірантів та молодих вчених, 25 березня 2014 р. : матер. конф. — Одеса, ОНЕУ. — С. 85-89.
316. Пархуць, Л. Інформаційні системи в освіті: автоматизовані навчальні системи [Текст] / Л. Пархуць, С. Ясинська // Гармонізація суспільства — новітній напрямок розвитку держави : Всеукр. наук. конф. аспірантів та молодих вчених, 25 березня 2014 р. : матер. конф. — Одеса, ОНЕУ. — С. 90-94.
317. Мінін, А. Інформаційні системи в освіті: електронний підручник [Текст] / А. Мінін, С. Ясинська // Гармонізація суспільства — новітній напрямок розвитку держави : Всеукр. наук. конф. аспірантів та молодих вчених, 25 березня 2014 р. : матер. конф. — Одеса, ОНЕУ. — С. 95-101.
318. Домаскін, О. Інформаційні системи в освіті: електронна енциклопедія [Текст] / О. Домаскін, С. Ясинська // Гармонізація суспільства — новітній напрямок розвитку держави : Всеукр. наук. конф. аспірантів та молодих вчених, 25 березня 2014 р. : матер. конф. — Одеса, ОНЕУ. — С. 102-108.
319. Буй, В. М. Інформаційні системи в освіті: електронна енциклопедія [Текст] / В. М. Буй, О. В. Орлик // Гармонізація суспільства — новітній

- напрямок розвитку держави : Всеукр. наук. конф. аспірантів та молодих вчених, 25 березня 2014 р. : матер. конф. — Одеса, ОНЕУ. — С. 109-116.
320. Єсіна, О. Г. Електронний підручник як засіб підвищення якості освіти [Текст] / О. Г. Єсіна, Л. М. Лінгур // Теорія та методика навчання фундаментальних дисциплін у вищій школі. — 2011. — № 2. — С. 255-260.
321. Єсіна, О. Г. Електронні підручники: переваги та недоліки використання [Текст] / О. Г. Єсіна, Л. М. Лінгур // Вісник соціально-економічних досліджень. — 2012. — Вип. 44 (1). — С. 181-186.
322. Єсіна, О. Г. Критерії оцінки якості підготовки сучасних фахівців [Текст] / О. Г. Єсіна // Теорія та методика навчання фундаментальних дисциплін у вищій школі. — 2012. — № 7. — С. 84-90.
323. Єсіна, О. Г. Вибір системи підтримки прийняття рішень в управлінні організацій [Текст] / О. Г. Єсіна, Л. М. Лінгур // Обліково-аналітичне забезпечення інноваційної трансформації економіки України : IV Всеукр. наук.-практ. Інтернет-конф., 21-25 травня 2010 р. : матер. конф. — Одеса : ОНПУ. — С. 180-182.
324. Єсіна, О. Г. Стратегія вибору системи підтримки прийняття рішень в управлінні підприємством [Текст] / О. Г. Єсіна, Л. М. Лінгур // Економіка: проблеми теорії та практики. — 2009. — № 256. — Т. 6. — С. 1438-1446.
325. Єсіна, О. Г. Программные продукты информационной безопасности бизнеса [Електронний ресурс] / О. Г. Єсіна, Л. М. Лінгур // Матеріали Сьомої Всеукраїнської науково — практичної Інтернет — конференції «Обліково-аналітичне забезпечення інноваційної трансформації економіки України» , Том 1 (Одеський національний політехнічний університет, 21-25 травня 2013). — Одеса : ОНПУ. — 2013. — С. 138-141. — Режим доступу [www/ URL: http://economics.opu.ua/files/science/2013/21.05/section_VI.pdf](http://www.economics.opu.ua/files/science/2013/21.05/section_VI.pdf). — Заголовок з контейнера, доступ вільний, 30.01.2014.
326. Єсіна, О. Г. Інтернет-банкінг в Україні: сучасний стан, проблеми та перспективи [Текст] / О. Г. Єсіна // Вісник соціально-економічних досліджень. — 2013. — Вип. 48 (1). — С. 209-213.
327. Петров, А. А. Автоматическая диагностика защищенности канала передачи данных на основании динамических измерений [Текст] / А. А. Петров // Захист інформації: — 2008. — № 40. — С. 77-80.
328. Петров, А. А. Использование сигналоподобных помех в системах активной защиты информации [Текст] / А. А. Петров // Інформаційна безпека. — 2010. — № 2(4). — С. 108-111.
329. Методологія та організація наукових досліджень. Практикум : навчальний посібник [Текст] / А. О. Петров, С. М. Головань, Ю. В. Полупан, Т. Л. Щербак. — Луганськ : СНУ ім. В. Даля, 2011. — 216 с.

330. Електронний документообіг за галуззю знань «Інформаційна безпека». Практикум : навчальний посібник / А. О. Петров, К. І. Белоусова, С. М. Головань, А. В. Мінін. — Луганськ : СНУ ім. В. Даля, 2011. — 260 с.
331. Petrov, A. Methods for troubleshooting of corporate network fault tolerance [Текст] / A. Petrov, M. Aleksander, K. Serhiyenyа // Вісник Східноукраїнського національного університету ім. В. Даля. — 2012. — № 8(179). — С. 348-355.
332. Петров А. А. Родной интерфейс программирования операционных систем Windows NT — NT Native API. Использование NT Native API для получения системной информации о процессах и потоках [Текст] / А. А. Петров, А. Г. Болдарев // Інформаційна безпека. — 2012. — № 1(7). — С. 55-64.
333. Петров, А. О. Моделі та методи розпізнавання мови [Текст] / А. О. Петров // Сучасний захист інформації. — 2012. — № 1. — С. 25-33.
334. Петров, А. О. Методичні вказівки до виконання лабораторних робіт з дисципліни «Системне програмне забезпечення. Частина перша» для студентів спеціальностей 6.050102 «Комп'ютерна інженерія», 6.170101 «Безпека інформаційних і комунікаційних систем» всіх форм навчання [Текст] / А. О. Петров, О. С. Зверева. — Луганськ : СНУ ім. В. Даля, 2012. — 64 с.
335. Петров, А. О. Методичні вказівки до виконання лабораторних робіт з дисципліни «Основи програмування мережевого середовища» для студентів спеціальностей 6.050102 «Комп'ютерна інженерія», 6.170101 «Безпека інформаційних і комунікаційних систем» всіх форм навчання [Текст] / А. О. Петров, О. С. Зверева. — Луганськ : СНУ ім. В. Даля, 2012. — 89 с.
336. Петров, А. О. Спеціальне діловодство. Практикум. [Текст] / А. О. Петров, К. І. Белоусова, С. М. Головань, А. В. Мінін [та ін.]. — Луганськ : СНУ ім. В. Даля, 2012. — 180 с.
337. Петров, А. О. Методичні вказівки до виконання курсового проектування з дисципліни «Захист комп'ютерних мереж» для студентів спеціальностей 6.050102 «Комп'ютерна інженерія», 6.170101 «Безпека інформаційних і комунікаційних систем» всіх форм навчання [Текст] / А. О. Петров, А. В. Мінін. — Луганськ : СНУ ім. В. Даля, 2012. — 37 с.
338. Петров, А. О. Методичні вказівки до виконання курсового проектування з дисципліни «Системне програмне забезпечення» для студентів спеціальності 6.170101 «Безпека інформаційних і комунікаційних систем» всіх форм навчання [Текст] / А. О. Петров, О. С. Зверева. — Луганськ : СНУ ім. В. Даля, 2012. — 51 с.
339. Скопа О.О. Интервальное оценивание надежности Т-систем с параллельным соединением элементов за результатами их биномиальных испытаний / Наукові праці ОНАЗ: Період. наук. збір. з радіотехніки і телекомунікацій, електроніки та економіки в галузі зв'язку. — Одеса, 2002. — №1. — С.65-71.

340. Панфилов И.П., Скопа А.А. Надежность работы линии связи, состоящей из основного и резервного каналов // Радиотехника: Всеукр. межведомств. научн.-техн. сб. — Харьков. — 2002. — Вып. 128. — С.91-96.
341. Скопа О.О. Оптимізація експлуатації резервних систем телекомунікацій // Праці УНДІРТ. — Одеса, 2002. — №1(29). — С.91-93.
342. Щербина, Ю. В. Принципи вибору формальних параметрів при побудові профілей захисту інфоресурсів [Текст] / Ю. В. Щербина, С. Л. Волков, О. О. Скопа // Восточно-Европейский журнал передовых технологий. ¾ 2012. ¾ №5/2(59). ¾ С. 31-33.
343. Скопа О.О. Статистичне тестування симетричних криптографічних перетворень / Східноєвропейський журнал передових технологій. Інформаційно-управляючі системи. — №4/9 (52), 2011. — Х.: Укр. акад. залізничн. транспорту, «Технологічний центр». — С.15-18.
344. Скопа А.А., Билык Н.М. Анализ влияния точности измерения параметров радиоканала на помехоустойчивость приема / Наукові записки УНДІЗ. — №1. — К.: УНДІЗ, 2007. — С.79-85.
345. Скопа О.О., Волков С.Л., Мінін А.В. Концепція контрольних випробувань резервних систем на основі біноміальної схеми / Інформаційна безпека. — №2(6), 2011. — Луганськ: СНУ ім. В.Даля. — С.69-76.
346. Скопа О.О. Інформатизація професійної діяльності фахівців // Актуальні проблеми держави і права: Зб. наук. праць. Вип. 25 / Редкол.: С.В.Ківалов (голов. ред.) та ін.; Відп. за вип. Ю.М. Оборотов. — Одеса: Юридична література, 2005. — С. 623-626.
347. Скопа О.О. Біноміальна схема контрольних випробувань резервних систем зв'язку // Зб. науков. праць УДМТУ. — Миколаїв: УДМТУ, 2002. — №7 (385). — С.116-124.
348. Скопа О.О. Інформаційні технології у професіональній діяльності фахівця / Наукові праці УДАЗ: Період. наук. збір. з радіотехніки і телекомунікацій, електроніки та економіки в галузі зв'язку. — Одеса, 2000. — №1. — С.103-106.
349. Wooldridge, M. J. Intelligent Agents: Theory and Practice [Текст] / M. J. Wooldridge, N. R. Jennings // The Knowledge Engineering Review. 1995.
350. Клышинский, Э. С. Некоторые аспекты построения агентных систем [Электронный ресурс] / Э. С. Клышинский // Портал : pmg.org.ru. — Режим доступа \www/ URL: <http://pmg.org.ru/russian/>. — Заголовок з контейнера, доступ умовно-вільний, 11.05.2012.
351. Wooldridge, M. J. Intelligent Agents [Текст] / M. J. Wooldridge // Multi-agent Systems. — 2001. — P. 27.
352. Wooldridge M. J. The logical modelling of computational multi-agent systems [Текст] / M. J. Wooldridge // A thesis submitted to the university of manchester for the degree of doctor of philosophy in the faculty of technology. — 163 p.

353. Shoham Y., Leyton-Brown K. Algorithmic, Game-Theoretic, and Logical Foundations. — London: Cambridge University Press, 2009 ; [Электронный ресурс] : Портал : Научная библиотека. — Режим доступа \www/ URL: http://science-library.at.ua/load/sistemy_iskusstvennogo_intellekta/multiagentnye_sistem_y/1_y_shoham_k_leyton_brown/ 5-1-0-1. — Заголовок з контейнера, доступ умовно-вільний, 18.08.2013.
354. Jennings, N. R. Applications of Intelligent Agents [Текст] / N. R. Jennings, M. J. Wooldridge // London : Queen Mary & Westfield College, University of London. — 2000. — 27 p.
355. Parunak, H. Industrial and Practical Application of DAI [Текст] / H. Parunak // Multiagent Systems. — 2001. — P. 27-79.
356. Openflow Switch Specification Version 1.4.0, August 5, 2013 [Электронный ресурс] / Портал : opennetworking.org. — Режим доступа \www/ URL: www.opennetworking.org. — Заголовок з екрану, доступ вільний, 22.02.2013.
357. Kim H., Feamster N. Improving network management with software defined networking // Communications magazine. IEEE, 2013. P. 114-119.
358. Al-Shaer E., Marrero W., El-Atawy A., El Badawi K. Network Configuration in a Box: Toward End-to-End Verification of Network Reachability and Security // 17th IEEE International Conference on Network Protocols (ICNP'09). Princeton, New Jersey, USA, 2009. P. 123-132.
359. Mai H., Khurshid A., Agarwal R., Caesar M., Godfrey R.B., King S.T. Debugging of the Data Plane with Anteatr // Proceedings of the ACM SIGCOMM conference. 2011. P. 290-301.
360. Kazemian P., Varghese G., Mckeown N. Header space analysis: Static checking for networks // Proceedings of 9-th USENIX Symposium on Networked Systems Design and Implementation. 2012.
361. Khurshid A., Zhou W., Caesar M., Godfrey P.B. Veriflow: Verifying Network-Wide Invariants in Real Time // Proceedings of International Conference «Hot Topics in Software Defined Networking»(HotSDN). 2012. P. 49-54.
362. Gutz S., Story A., Schlesinger C., Foster N. Splendid isolation: A Slice Abstraction for Software Defined Networks // Proceedings of International Conference «Hot Topics in Software Defined Networking» (HotSDN). 2012. P. 79-84.
363. Reitblatt M., Foster N., Rexford J., Walker D. Consistent updates for software-defined networks: change you can believe in! // Hotnets. 2011. V. 7.
364. Reitblatt M., Foster N., Rexford J., Schlesinger C., Walker D. Abstractions for Network Update // Proceedings of ACM SIGCOMM conference. 2012. P. 323-334.

365. Canini M., Venzano D., Peresini P., Kostic D., Rexford J. A NICE way to Test Openflow Applications // Proceedings of Networked Systems Design and Implementation, April 2012.
366. Immerman N. Languages that capture complexity classes // SIAM Journal of Computing. 1987. V. 16, No 4. P. 760-778.
367. Immerman N., Vardi M. Model checking and transitive closure logic // Lecture Notes in Computer Science. 1997. P. 291-302.
368. Alechina N., Immerman N. Reachability logic: efficient fragment of transitive closure logic // Logic Journal of IGPL. 2000. V. 8, No 3. P. 325-337.
369. Корчинський, В. В. Оцінка структурної скритності сигнальних конструкцій на основі хаотических сигналів в системах передачі конфіденціальної інформації [Текст] / В. В. Корчинський // Збірник наукових праць ОНАЗ ім. О. С. Попова. — 2012. — № 2. — С. 77-83
370. Управление информационными потоками сетей радиосвязи в условиях радиозлектроного противодействия [Текст] : автореферат дис. ... канд. техн. наук : 05.13.01 / Е. А. Шабалин ; НГТУ им. Р.Е. Алексеева. — Нижний Новгород : [б. и.], 2008. — 17 с.
371. Корчинський, В. В. Умовне забезпечення енергетическої скритності хаотических сигналів при передачі конфіденціальної інформації [Текст] / В. В. Корчинський, Н. Ф. Казакова // Сучасний захист інформації. — 2013. — № 3. — С. 12-17.
372. Корчинський, В. В. Умовне забезпечення енергетическої скритності хаотических сигналів при передачі конфіденціальної інформації [Текст] / В. В. Корчинський, Н. Ф. Казакова, В. О. Манько // Збірник наукових праць Одеської державної академії технічного регулювання та якості. — 2013. — № 2(3). — С. 27-32.
373. Захарченко, Н. В. Скритність передачі в системах зв'язу з хаотическими сигналами [Текст] / Н. В. Захарченко, С. М. Горохов, В. В. Корчинський, Б. К. Радзимовський // Вимірювальна та обчислювальна техніка в технологічних процесах. — 2013. — №3. — 161-164.
374. Гуляев, Ю. В. Информационные технологии на основе динамического хаоса для передачи, обработки, хранения и защиты информации [Текст] / Ю. В. Гуляев, Р. В. Беляев, Г. М. Воронцов [и др.] // Радиотехника и электроника. — 2003. — Т. 48. — № 10. — С. 1157-1165.
375. Корчинський, В. В. Модель шумового сигналу для передачі конфіденціальної інформації [Текст] / В. В. Корчинський // Вестник НТУ «ХПИ». — 2013. — № 11(985). — С. 89-94.
376. Корчинський, В. В. Метод моделювання шумових сигналів для систем передачі конфіденціальної інформації [Текст] / В. В. Корчинський // Вестник НТУ «ХПИ». — 2013. — № 38(1011). — С. 99-105.
377. Розвиток теорії та методів випробування захищеності інформаційно-комунікаційних систем та мереж [Текст] : дис... докт. техн. наук :

- 05.13.21 / Скопа Олександр Олександрович; НУ «Львівська політехніка». — Львів, 2011. — 358 с. (ДСК).
378. Головань, В. Г. Методика использования последовательностей для повышения безопасности компьютерных радиосетей, построенных на принципах кодового разделения каналов [Текст] / В. Г. Головань, Н. Ф. Казакова // Комп'ютерні технології, інформаційна безпека та дизайн : IV наук.-практ. конф. проф.-викл. складу та студентства Міжнародного гуманітарного ун-ту, 22 травня 2009 р. : матер. конф. — Одеса, МГУ — С. 80-82.
379. Головань, В. Г. Послідовність на основі слідів полів Галуа [Текст] / В. Г. Головань, Н. Ф. Казакова // Захист інформації. — 2008. — Спец. випуск (40). — С. 95-100.
380. Казакова, Н. Ф. Синтез алгоритму роботи та технічна реалізація декомпозиційного генератора послідовності [Текст] / Н. Ф. Казакова // Захист інформації. — 2009. — № 1(42). — С. 86-89.
381. Билык, Н. М. Анализ алгоритмов формирования датчиков псевдослучайных чисел с равномерным распределением [Текст] / Н. М. Билык, Н. Ф. Казакова // Наукові записки УНДІЗ. — 2009. — № 2(10). — С. 103-106.
382. Казакова, Н. Ф. Инструментальные средства для предварительного анализа криптографических программных генераторов ПСП [Текст] / Н. Ф. Казакова, Ю. В. Щербина // Сучасний захист інформації. — 2010. — № 1. — С. 31-35.
383. Казакова, Н. Ф. Поэтапное тестирование и подбор составных элементов генераторов псевдослучайных последовательностей [Текст] / Н. Ф. Казакова // Восточно-европейский журнал передовых технологий. — 2010. — № 2/8(44). — С. 44-48.
384. Казакова, Н. Ф. Статистическое тестирование криптографических генераторов [Текст] / Н. Ф. Казакова, Ю. В. Щербина // Вісник Східноукраїнського національного університету імені Володимира Даля. — 2010. — № 9(151). — Т. 1. — С. 29-36.
385. Казакова, Н. Ф. Частотное тестирование криптографических генераторов псевдослучайных последовательностей [Текст] / Н. Ф. Казакова, Ю. В. Щербина // Сучасний захист інформації. — 2010. — № 3. — С. 51-57.
386. Казакова, Н. Ф. Аналіз стану розвитку інструментальних засобів для тестування вихідних послідовностей симетричних шифрувальних пристроїв [Текст] / Н. Ф. Казакова, Ю. В. Щербина // Метрологія та прилади. — 2011. — № 4(30). — С. 27-30.
387. Щербина, Ю. В. Обобщение результатов тестирования генераторов псевдослучайных последовательностей [Текст] / Ю. В. Щербина, Н. Ф. Казакова // Інформаційна безпека. — 2012. — № 1(7). — С. 90-95.
388. Казакова, Н. Ф. Проблемы оценки качества работы современных линейных генераторов псевдослучайных последовательностей [Текст] /

- Н. Ф. Казакова, Ю. В. Щербина // Збірник наукових праць Одеської державної академії технічного регулювання та якості. — 2013. — № 1(2). — С. 32-36.
389. Казакова, Н. Ф. Проблемы построения комбинированных линейных генераторов псевдослучайных чисел [Текст] / Н. Ф. Казакова, Ю. В. Щербина // Інформаційна безпека. — 2013. — № 2(10). — С. 58-64.
390. Казакова, Н. Ф. Аналитическое обоснование использования gfsr-генераторов в задачах криптографии [Текст] / Н. Ф. Казакова // Технологічний аудит та резерви виробництва. — 2013. — № 5/5(12). — С. 45-47.
391. Казакова, Н. Ф. Елементи практичної реалізації частотного тесту генераторів криптографічних перетворень // Удосконалення принципів та методів інформаційного забезпечення, інформаційної та фінансово-економічної безпеки підприємств та організацій сфери економіки, бізнесу та фінансів [Звіт про НДР] : (пром.жн.) / О. О. Скопа, Н. Ф. Казакова, О. В. Орлик, Ю. В. Щербина, А. О. Петров, С. Л. Волков, О. І. Мацків, О. Г. Єсіна, А. Ю. Вакула, О. О. Фразе-Фразенко, А. В. Мінін, О. О. Йона, Є. В. Вавілов, К. Б. Айвазова ; кер. О. О. Скопа. — Одеса : ОНЕУ, 2013. — 0112U007713. — 236 с. — С. 127-136
392. Казакова, Н. Ф. Программная реализация универсального статистического теста Маурера для анализа псевдослучайных последовательностей [Текст] / Н. Ф. Казакова, Ю. В. Щербина // Вісник Східноукраїнського національного університету імені Володимира Даля. — 2011. — № 7(161). — Т. 1. — С. 289-296.
393. Шаньгин, А. И. Информационная безопасность компьютерных систем и сетей [Текст] : монография / А. И. Шаньгин. — М. : ИД «Форум»: Инфра-М, 2008. — 416 с.: ил.
394. Цифровий прецизійний часовий дискримінатор [Текст] : пат. 84575 Україна : МПК (2013.01) H03D 13/00 / Коваль В. В., Костік Б. Я., Лисенко В. П., Казакова Н. Ф. ; заявник та патентообладач Національний університет біоресурсів і природокористування України ; заявл. 19.04.2013 ; опубл. 25.10.2013, бюл. № 20.
395. Kazakova, N. Mobil radio-service management system construction principles [Текст] // Proceeding of the International Conference TCSET'2002 «Modern Problems of Radio Engineering, Telecommunications and Computer Science»: February 18-23, 2002. — Lviv-Slavsk, Ukraine: Lviv Polytechnic National University — IEEE Networking the World. — 2002. — P. 284.
396. Казакова, Н. Ф. Принципи побудови захищених інтелектуальних мереж [Текст] / Н. Ф. Казакова // Наукові записки Міжнародного гуманітарного університету. — 2008. — № 14. — С. 69-75.
397. Скопа, О. О. Системний аналіз особливостей впровадження захищених інформаційних мереж в Україні та синтез критерію їх ефективності [Текст] / О. О. Скопа, Н. Ф. Казакова // Наукові записки

- Міжнародного гуманітарного університету. — 2009. — № 16. — С.115-122.
398. Казакова, Н. Ф. Анализ принципиальной задачи факторизации модели отказа предоставления услуги в сети NGN на уровне управления сетью [Текст] / Н. Ф. Казакова, В. И. Гура // Інформаційна безпека. — Луганськ : СНУ ім. В. Даля. — 2010. — № 1(3). — С. 127-131.
399. Скопа О.О., Вавілов Є.В. Інтелектуальні автономні системи: концептуальні положення створення та функціонування / Бионика интеллекта. — №1(80), 2013. — Харьков: ХНУРЭ. — С. 35-40..
400. Панфилов В.И., Скопа А.А. Синтез частотных цифровых приемников для защищенных радиосистем / Захист інформації. — №7(4), 2009. — К.: ДУІКТ. — С.361-369.
401. Ali S. Dakdouki, Victor L. Banket, Nikolai K. Mykhaylov, Alexander A. Skopa. Downlink Processing Algorithms for Multi-Antenna Wireless Communications. — IEEE Communication Magazine, January, 2005. — Vol. 43, №1. — pp.122-127.
402. Казакова, Н. Ф. Управління послугами телекомунікацій [Текст] / Н. Ф. Казакова // II звітн. наук.-практ. конф. проф.-викл. складу та студентства Міжнародного гуманітарного університету, 12 квітня 2007 р. : матер. конф. — МГУ, Одеса. — С. 18-21.
403. Казакова, Н. Ф. Раціональна концепція інтелектуальної мережі як предмет протиріччя [Текст] / Н. Ф. Казакова // Комп'ютерні технології, інформаційна безпека та дизайн : IV наук.-практ. конф. проф.-викл. складу та студентства Міжнародного гуманітарного університету (секції 7...13), 22 травня 2009 р. : матер. конф. — МГУ, Одеса. — С. 126-128.
404. Казакова, Н. Ф. Априорна суперечність раціональної концепції інтелектуальної мережі [Текст] / Управління проектами: стан та перспективи : міжнар. наук.-техн. конф., 2009 : матер. конф. — НУК ім. адмірала Макарова, Миколаїв. — С. 65-67.
405. Дроздов, В. А. Применение игрового подхода к анализу информационной безопасности [Текст] / В. А. Дроздов, В. Г. Головань, А. В. Головань, Н. Ф. Казакова // Современные информационные и электронные технологии СИЭТ-2009 : X міжнар. наук.-практ. конф., 18-22 травня 2009 р. — ОдНПУ, Одесса. — С. 69.
406. Petrov, A. Analiza stanu bezpieczeństwa ekonomicznego w sferze nowoczesnej ekonomii i biznesu [Текст] / Anton Petrov, Mikołaj Karpiński, Nadiya Kazakova // Zeszyty Naukowe Wyższej Szkoły Finansów i Prawa. — Bielsko-Biała : Wyższa Szkoła Finansów i Prawa. — 2013. — № 4. — S. 27-38.
407. Казакова, Н. Ф. Влияние информационных технологий на общественное сознание и образование [Текст] / Н. Ф. Казакова, А. А. Скопа // Наукові записки Міжнародного гуманітарного університету. — 2004. — № 1. — С. 39-47.

408. Казакова, Н. Ф. Аналіз напрямів розвитку інформаційної безпеки у комп'ютерних системах та мережах на основі застосування програмних засобів захисту інформації [Текст] / Н. Ф. Казакова // Вісник Львівського національного аграрного університету: Агроінженерні дослідження. — Львів : ЛНАУ. — 2010. — № 14. — С. 47-57.
409. Казакова Н. Ф. Моніторинг інформаційних ресурсів в захищених інформаційних мережах / Н. Ф. Казакова // «Світ інформації та телекомунікацій» : VII Міжнар. наук.-техн. конф. студентства та молоді, 15-16 квітня 2010 р. : матер. конф. — Київ : ДУІКТ. — С. 165-168.
410. Kazakova N. Mathematical models for the reliability research // Proceedings of the VIIth International Conference CADSM'2003 «The Experience of Designing and Application of CAD Systems of Microelectronics»: February 18-23, 2003. — Lviv-Slavske, Ukraine: Lviv Polytechnic National University — IEEE Networking the World. — 2003. — С.388.
411. Герасименко, В. А. Защита информации в автоматизированных системах обработки данных : в 2-х кн. [Текст] / В. А. Герасименко. — М. : Энергоатомиздат, 1994. — Т. 1. — С. 132-138.
412. Борисов, А. Н. Принятие решения на основе нечетких моделей: примеры использования [Текст] / А. Н. Борисов, О. А. Крумберг, И. П. Федоров. — Рига : Знание, 1990. — 184 с.
413. Домарев, В. В. Безопасность информационных технологий. Системный подход [Текст] / В. В. Домарев. — К. : ТОВ «ТВД ДС», 2004. — 992 с.
414. Лахно, В. А. Построение дискретных процедур распознавания и поиска уязвимостей информации [Текст] / В. А. Лахно, А. С. Петров, А. С. Скрипкина // Інформаційна безпека. — 2010. — №2(4). — С. 5-13.
415. Pearson, K. On the criterion that a given system of deviations from the probable in the case of a correlated system of variables is such that it can reasonably be supposed to have arisen from random sampling / K. Pearson // Phil. Mag., 1900, V. 50, P. 157-175.