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***

«___»_____2013 г.

ЗВІТ

про науково-дослідну роботу

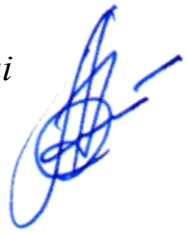
УДОСКОНАЛЕННЯ ПРИНЦИПІВ ТА МЕТОДІВ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ, ІНФОРМАЦІЙНОЇ ТА ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ ТА ОРГАНІЗАЦІЙ СФЕРИ ЕКОНОМІКИ, БІЗНЕСУ ТА ФІНАНСІВ

(проміжний)

Рукопис закінчено 1 грудня 2013 року

Науковий керівник НДР

завідувач кафедри Інформаційних систем в економіці
докт. техн. наук, доцент



О.О. Скопа

Одеса – 2013

СПИСОК ВИКОНАВЦІВ

Науковий керівник
докт. техн. наук, доцент — О.О. Скопа
(вступ, підрозділи 1.1-1.5, 3.5, висновки до звіту)

Відповідальний виконавець
канд. техн. наук., доцент — Н.Ф. Казакова
(підрозділи 3.1, 3.3, 3.4, висновки до розділів)

Виконавці

канд. екон. наук, доцент — О.В. Орлик
(підрозділ 2.3)

канд. техн. наук, доцент — Ю.В. Щербина
(підрозділ 3.1)

канд. техн. наук, доцент — А.О. Петров
(підрозділ 3.2)

канд. техн. наук, доцент — С.Л. Волков
(підрозділи 3.5, 3.6)

канд. екон. наук, ст. викладач — О.І. Мацків
(підрозділ 2.5)

ст. викладач — О.Г. Єсіна
(підрозділи 2.1, 2.2)

ст. викладач — А.Ю. Вакула
(підрозділ 2.6)

ст. викладач — О.О. Фразе-Фразенко
(підрозділи 1.6, 1.7)

ст. викладач — А.В. Мінін
(підрозділ 3.3)

викладач — О.О. Йона
(підрозділ 2.4)

аспірант — Є.В. Вавілов
(підрозділ 3.6)

аспірант — К.Б. Айвазова
(підрозділ 3.7)

У зборі та обробці інформації приймали участь студенти: кредитно-економічного факультету: Д. Осипенко (розрахунки до підрозділу 3.4), В. Педько (пошук літератури до розділу 1), А. Білодон (оформлення списку літературних першоджерел); факультету економіки та управління підприємством: В. Капацина та М. Панкрашева (пошук літератури до розділів 2 та 3); обліково-економічного факультету: В. Ліске та о. Александров (розрахунки до підрозділу 3.6); факультету міжнародної економіки: А. Маліченко, К. Вишемірська та К. Білоус (розрахунки до розділу 3).

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, 3 розділів з висновками, загального висновку до роботи, списку використаних літературних джерел та 1 додатку. Робота викладена на 236 сторінках, містить 221 сторінку основного тексту з 6 таблицями та 37 рисунками (з них 10 – на окремих сторінках) та списком використаних літературних джерел з 119 найменувань на 12 сторінках, 1 додаток на 3 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 пропонованих 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 у виданій монографії за темою дослідження, можуть бути використані при підготовці бакалаврів 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, невизначеність, надійність, генетичний алгоритм

ЗМІСТ

Стор.

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 унеможливлюється 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 завдавати 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 політичної 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 підприєствами 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 спіробітників 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.

РОЗДІЛ 1
ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. УПРАВЛІННЯ ІДЕНТИФІКАЦІЙНОЮ ІНФОРМАЦІЄЮ І ДОСТУПОМ

1.1. Сутність та поняття інформаційної безпеки підприємства

Поняття інформаційної безпеки, в залежності від його використання, розглядається в декількох ракурсах.

У загальному випадку інформаційна безпека – це стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використання і розвиток в інтересах громадян, організацій, держави.

Під *інформаційним середовищем* (англ.: *information environment*) розуміють сферу діяльності суб'єктів, пов'язану зі створенням, перетворенням і споживанням інформації. Інформаційне середовище умовно ділиться на три основні предметні частини:

– створення та розповсюдження вихідної та похідної інформації;

– формування інформаційних ресурсів, підготовки інформаційних продуктів, надання інформаційних послуг;

– споживання інформації,

і дві забезпечувальні предметні частини:

– створення і застосування інформаційних систем, інформаційних технологій та засобів їх забезпечення;

– створення і застосування засобів і механізмів інформаційної безпеки.

Більш *розгорнуте формулювання інформаційної безпеки* – це стан захищеності потреб в інформації особистості, суспільства та держави, при якому забезпечується їх існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз.

Слід зазначити, що задоволення в будь-якому ступені потреб в інформації призводить до оволодіння відомостями про навколишній світ і процеси,

що протікають в ньому, тобто інформованості особистості, суспільства і держави.

Стан інформованості визначає ступінь адекватності сприйняття суб'єктами навколишньої дійсності і, як наслідок, обґрунтованість рішень і дій, які приймаються [1, 12].

Залежно від виду загроз інформаційну безпеку можна розглядати наступним чином:

– як забезпечення стану захищеності особистості, суспільства, держави від впливу неякісної інформації;

– інформації та інформаційних ресурсів від неправомірного впливу сторонніх осіб;

– інформаційних прав і свобод громадянина.

В інформаційному праві інформаційна безпека – це одна із сторін розгляду інформаційних відносин у рамках інформаційного законодавства з позицій захисту життєво важливих інтересів особистості, суспільства, держави і акцентування уваги на погрози, механізми усунення або запобігання таких загроз правовими методами [1, 10, 11].

Питання інформаційної безпеки, які наведені в юридичній та спеціальній літературі, і базуються на розумінні інформаційної безпеки як складової національної безпеки України.

По суті це є вірним, оскільки завданням заходів з інформаційної безпеки є мінімізація шкоди за неповноти, несвоєчасність або недостовірність інформації чи негативного інформаційного впливу через наслідки функціонування інформаційних технологій, а також несанкціоноване поширення інформації [2, 13, 14]. Саме тому інформаційна безпека передбачає наявність певних державних інститутів і умов існування її суб'єктів, встановлених міжнародним і вітчизняним законодавством [3].

Крім цього, інформаційна безпека повинна забезпечуватися шляхом проведення цілісної державної програми відповідно до Конституції та чинного законодавства України і норм міжнародного права шляхом реалізації від-

повідних доктрин, стратегій, концепцій і програм, що стосуються національної інформаційної політики України [10, 11].

Підводячи підсумок, можна стверджувати, що інформаційна безпека має на увазі можливість безперешкодної реалізації суспільством і окремими його членами своїх конституційних прав, пов'язаних з можливістю вільного одержання, створення і поширення інформації. Поняття інформаційної безпеки слід також розглядати в контексті:

– забезпечення безпечних умов існування інформаційних технологій, що включають питання захисту інформації;

– інформаційної інфраструктури держави;

– інформаційного ринку та створення умов існування і розвитку інформаційних процесів.

Необхідний рівень інформаційної безпеки забезпечується сукупністю політичних, економічних, організаційних заходів, спрямованих на попередження, виявлення і нейтралізацію тих обставин, факторів і дій, які можуть надійти збиток або перешкодити реалізації інформаційних прав, потреб та інтересів країни та її громадян.

1.2. Методи забезпечення безпеки інформації підприємства

Форми і способи забезпечення інформаційної безпеки утворюють власне інструмент, за допомогою якого засоби інформаційної безпеки вирішують весь комплекс завдань із захисту життєво важливих інтересів підприємств та організацій сфери економіки, бізнесу та фінансів. Тому необхідно чітке юридичне оформлення при розробці нормативних актів, що регулюють діяльність органів інформаційної безпеки.

Найважливіша вимога до обґрунтування способів, форм та механізмів їх реалізації полягає в абсолютному верховенстві права в будь-якій діяльності. У свою чергу, кожен суб'єкт інформаційного процесу повинен мати відповідне правове свідомість, бути законослухняним, добре уявляти наслідки своїх

дій для інших суб'єктів і міру відповідальності на випадок порушення їх життєво важливих інтересів. Це є принциповим, оскільки застосування тих чи інших форм і способів залежить від того, є інформаційні загрози наслідком ненавмисних або умисних дій суб'єктів інформаційного процесу. У першому випадку забезпечення інформаційної безпеки здійснюється відповідно у формах інформаційного патронату та інформаційної кооперації, у другому – у формі інформаційного протиборства. Друга форма у рамках НДР не розглядається

Інформаційний патронат (лат.: *patronatys* від *patronys* – «захисник») – форма забезпечення інформаційної безпеки фізичних і юридичних осіб з боку держави. Він передбачає забезпечення органів управління системи інформаційної безпеки держави відомостями про дестабілізуючі фактори та загрози стану інформованості фізичних і юридичних осіб (інформаційне забезпечення інформаційної безпеки) і власне захист життєво важливих інтересів цих осіб від інформаційних загроз або, як ще кажуть, – інформаційний захист [4]. При цьому інформаційне забезпечення інформаційної безпеки (англ.: *information support of information security*) включає збір (добування) відомостей про дестабілізуючі фактори та інформаційні загрози, їх обробку, обмін інформацією між органами управління та силами і засобами системи інформаційної безпеки. Його основу складає збір (добування) необхідних відомостей, здійснюване в процесі розвідувальної, контррозвідувальної, оперативно-розшукової та оперативно-інформаційної діяльності.

Інформаційний захист (англ.: *infosecurity*) досягається шляхом внесення в порядку законодавчої ініціативи законопроектів, здійснення судового захисту, проведення оперативних заходів силами і засобами інформаційної безпеки.

Інформаційна кооперація (англ.: *information cooperation*; лат.: *cooperatio*, від *coopero* – «співпрацюю») – форма забезпечення інформаційної безпеки між рівноправними суб'єктами інформаційного процесу (фізичними, юридичними, міжнародними), який включає сукупність їх взаємоузгоджених дій,

спрямованих на отримання відомостей про дестабілізуючі фактори, дестабілізуючі та інформаційні загрози і захист від них доступними законними способами і засобами.

Для конкретної підприємств та організацій сфери економіки, бізнесу та фінансів такими способами і засобами можуть бути:

– судовий захист прав і свобод у використанні інформації;

– адміністративний захист її життєво важливих інтересів інформованості з боку територіальних або відомчих органів інформаційної безпеки;

– автономний захист своїх прав і свобод та комерційної таємниці, в основному із застосуванням технічних засобів захисту.

Це ж характерно і для громадських об’єднань та кожної окремої особи. Разом з тим, за наявності у них власних органів інформаційної безпеки, їх можливості у сфері автономного захисту істотно розширюються [5].

Проблеми захисту інформації в автоматизованих системах підприємств та організацій сфери економіки, бізнесу та фінансів виявилися практично одночасно з початком використання коштів електронної обчислювальної техніки при регулярної обробки інформації. Таким чином, історія захисту інформації обчислюється майже 40-річним періодом.

При застосуванні обчислювальної техніки для обробки інформації основна увага приділялася забезпеченню її фізичної цілісності та достовірності (надійності) інформації. У цьому зв’язку особливо слід відзначити той факт, що вітчизняна школа вчених і фахівців внесла істотний внесок у дослідження і вирішення цієї проблеми. Порушення цілісності інформації на цьому початковому етапі розвитку розглядалося як результат впливу природних факторів, головними з яких є відмови, збої і помилки елементів систем обробки.

Що стосується захисту від несанкціонованого отримання інформації, то вважалося, що автономність роботи ЕОМ перших поколінь, індивідуальність алгоритмічної реалізації процедур обробки, представлення інформації в пам’яті ЕОМ і на машинних носіях у закодованому вигляді, а також відносна простота організаційного контролю всього процесу обробки забезпечують

надійний захист інформації від несанкціонованого доступу до неї осіб, які не мають відповідних повноважень. Однак у міру розвитку самої обчислювальної техніки та інформаційних технологій, форм, способів і масштабів використання автоматизованої обробки інформації зазначені фактори втратили свою ефективність. У силу цього уразливість інформації з боку зловмисників стала цілком реальною, що й знайшло своє підтвердження в конкретних формах несанкціонованого отримання інформації, причому перші відомості про такі факти з'явилися у пресі більше двадцяти років тому.

Збиток від подібних дій нерідко набуває значних розмірів і приводить до дуже серйозних наслідків. Як приклад, можна навести несанкціоноване копіювання інформації, що є чиєюсь власністю. Останнім часом ці проблеми обговорюються досить інтенсивно, особливо, в першу чергу, щодо розкрадання програм для ЕОМ та використання у корисних цілях інформації, яка циркулює на підприємствах сфери економіки, бізнесу та фінансів. Про поширеність даного виду незаконних дій досить переконливо говорить хоча б такий факт: як стверджують зарубіжні фахівці, на кожну копію програми, отриману законним шляхом, існує не менше десяти копій, отриманих незаконним шляхом.

Можна навести велику кількість та інших конкретних прикладів злочинних дій по відношенню до інформації, що знаходиться в автоматизованих системах. Найбільш поширеною і небезпечною формою таких дій останнім часом виявилося зараження інформаційно-обчислювальних систем і мереж так званими комп'ютерними вірусами.

Згідно з визначенням, комп'ютерна безпека залежить не тільки від комп'ютерів, але і від підтримуючої інфраструктури, до якої можна віднести системи електропостачання, життєзабезпечення, вентиляції, засоби комунікацій, а також обслуговуючий персонал [6].

1.3. Основні складові інформаційної безпеки

Інформаційна безпека – багатогранна, багатовимірна область діяльності, в якій успіх може принести тільки систематичний, комплексний підхід.

Спектр інтересів суб'єктів, пов'язаних з використанням інформаційних систем, щодо інформаційних ресурсів і підтримуючої інфраструктури можна розділити на такі категорії:

– забезпечення доступності;

– забезпечення цілісності;

– забезпечення конфіденційності.

Іноді в число основних складових інформаційної безпеки включають *захист від несанкціонованого копіювання інформації*.

Доступність – це можливість за прийнятний час отримати необхідну інформаційну послугу. Під *цілісністю* мається на увазі актуальність інформації, її захищеність від руйнування і несанкціонованого зміни. Нарешті, *конфіденційність* – це захист від несанкціонованого доступу до інформації.

Інформаційні системи створюються (купуються) для отримання певних інформаційних послуг. Якщо з тих чи інших причин надати ці послуги користувачам стає неможливо, це, очевидно, завдає збитку всім суб'єктам інформаційних відносин. Тому, не протиставляючи доступність решті аспектів, ми виділяємо її як найважливіший елемент інформаційної безпеки.

Особливо яскраво провідна роль доступності виявляється в системах управління – на виробництві, транспорті і т.п. Зовні менш драматичні, але також неприємні наслідки – і матеріальні, і моральні – може мати тривала недоступність інформаційних послуг, якими користується велика кількість людей (продаж залізничних та авіаквитків, банківські послуги тощо).

Цілісність можна поділити на статичну (що розуміється як незмінність інформаційних об'єктів) і динамічну (що відноситься до коректного виконання складних дій (транзакцій)). Засоби контролю динамічної цілісності за-

стосовуються, зокрема, при аналізі потоку фінансових повідомлень з метою виявлення крадіжки, переупорядковування або дублювання окремих повідомлень.

Цілісність виявляється найважливішим аспектом інформаційної безпеки в тих випадках, коли інформація служить «керівництвом до дії». Рецептура ліків, наказані медичні процедури, набір і характеристики комплектуючих виробів, хід технологічного процесу на підприємствах та в організаціях сфери економіки, бізнесу та фінансів – все це приклади інформації, порушення цілісності якої може бути в буквальному сенсі життєво важливим.

Неприємно і спотворення офіційної інформації, будь то текст закону або сторінка Web-сервера-якої урядової організації або дані банківської структури.

На жаль, практична реалізація заходів щодо забезпечення конфіденційності сучасних інформаційних систем натрапляє на серйозні труднощі.

По-перше, відомості про технічні канали витоку інформації є закритими, так що більшість користувачів позбавлені можливості скласти уявлення про потенційні ризики.

По-друге, на шляху користувальницької криптографії, як основного засобу забезпечення конфіденційності, стоять численні законодавчі перепони і технічні проблеми. Якщо повернутися до аналізу інтересів різних категорій суб’єктів інформаційних відносин, то майже для всіх, хто реально використовує Інформаційні Системи, на першому місці стоїть доступність.

Практично не поступається їй за важливістю цілісність – який сенс в інформаційній послузі, якщо вона містить спотворені відомості? Нарешті, конфіденційні моменти є також у багатьох організацій (навіть у різних навчальних інститутах намагаються не розголошувати відомості про зарплату співробітників) і окремих користувачів (наприклад, паролі) [6].

1.4. Організація системи інформаційної безпеки підприємства

1.4.1. Правила побудови системи інформаційної безпеки підприємства

Підприємства та організації сфери економіки, бізнесу та фінансів (далі – *підприємства*) – найбільш численні структури, в яких створюється найбільший обсяг (кількість) інформації, яка містить державну і конфіденційну таємницю. У них проводиться конкретна і різноманітна робота по захисту інформації. Система інформаційної безпеки підприємства повинна базуватися на принципах, які зазначені нижче.

Профілактика можливих загроз. Необхідне своєчасне виявлення можливих загроз безпеки підприємства, аналіз яких дозволить розробити відповідні профілактичні заходи.

Законність. Заходи щодо забезпечення безпеки розробляються на основі і в рамках чинних правових актів(наприклад, [10, 11]). Локальні правові акти підприємства не повинні суперечити законам і підзаконним актам.

Комплексне використання сил і засобів. Для забезпечення безпеки використовуються всі наявні в розпорядженні підприємства сили та засоби. Кожен співробітник повинен, в рамках своєї компетенції, брати участь у забезпеченні безпеки підприємства. Організаційною формою комплексного використання сил і засобів є програма (план робіт) забезпечення безпеки підприємства.

Координація та взаємодія всередині і поза підприємством. Заходи протидії загрозам здійснюються на основі взаємодії та координації зусиль усіх підрозділів, служб підприємства, а також встановлення необхідних контактів із зовнішніми організаціями, здатними надати необхідне сприяння в забезпеченні безпеки підприємства. Організувати координацію і взаємодію всередині і поза підприємства може служба безпеки (СБ) підприємства (або керівник підприємства, якщо СБ в організації немає).

Поєднання гласності з секретністю. Доведення інформації до відома персоналу підприємства та громадськості в допустимих межах заходів безпеки виконує найважливішу роль – запобігання потенційних і реальних загроз.

Компетентність. Співробітники повинні вирішувати питання забезпечення безпеки на професійному рівні, а в необхідних випадках спеціалізуватися по основним його напрямками.

Економічна доцільність. Вартість фінансових витрат на забезпечення безпеки не повинна перевищувати той оптимальний рівень, при якому втрачається економічний сенс їх застосування.

Планова основа діяльності. Діяльність щодо безпеки повинна будуватися на основі комплексної програми забезпечення безпеки підприємства, підпрограм забезпечення безпеки по основних його видами (економічна, науково-технічна, екологічна, технологічна і т.д.) і розроблюваних для їх виконання планів роботи підрозділів підприємства та окремих співробітників.

Системність. Цей принцип передбачає врахування всіх факторів, що впливають на безпеку підприємства, включення діяльність щодо його забезпечення всіх співробітників, використання всіх сил і засобів [7].

1.4.2. Принципи захисту інформації

Забезпечення інформаційної безпеки – це сукупність заходів, призначених для досягнення стану захищеності потреб особистостей, суспільства і держави в інформації. У випадку, який є предметом дослідження у НДР – підприємства та організації сфери економіки, бізнесу та фінансів.

Держава здійснює свої заходи через відповідні органи, а громадяни, громадські організації та об’єднання, що мають відповідні повноваження, – відповідно до законодавства. В основу забезпечення інформаційної безпеки підприємств та організацій сфери економіки, бізнесу та фінансів, як і держави в цілому, мають бути покладені такі принципи:

– законність, дотримання балансу інтересів особи, суспільства і держави;

– взаємна відповідальність суб'єктів забезпечення інформаційної безпеки;

– інтеграція систем національної та міжнародної безпеки.

Специфічними принципами забезпечення інформаційної безпеки є:

– превентивний характер проведення її заходів щодо заходів інших видів безпеки;

– адекватна інформованість об'єктів безпеки, в тому числі і міжнародних.

Превентивність (лат.: *praeventio* від *praevenio* – «попереджаю») обумовлена властивою людині послідовністю виконання операцій, що становить будь-яку елементарну дію. Все починається з прийому (добування) інформації, а закінчується активною дією: реакцією на отриману інформацію. Оскільки це справедливо відносно будь-якого виду діяльності, то можна стверджувати, що даний принцип є загальним, і його дія поширюється як на всі сфери безпеки особистості, суспільства і держави, так і на конкретні підприємства та організації.

Адекватна інформованість об'єктів безпеки означає, що всі вони мають право володіти інформацією про явища і процеси , які їх цікавлять, яке обмежене тільки законодавчо з метою охорони професійної, комерційної та державної таємниці [8].

Права і свободи суспільства в питаннях пошуку, володіння і розповсюдження інформації повинні регулюватися законодавчими актами, які видаються, про специфіку діяльності громадських об'єднань та організацій або про зміст інформації. Наприклад, адекватна інформованість суспільства про його матеріальні цінності досягається у сфері нормотворчості і правозастосування законодавства про захист комерційної таємниці. Права і свободи суспільства в духовній сфері мають захищати законодавчі акти, що визначають порядок утворення і функціонування освітніх, просвітницьких, культурних, релігійних організацій, а також ЗМІ. В основі прав і свобод держави у сфері її інформованості з питань світової політики, економіки, науки, ресурсів, еко-

логії, оборони і т.д. лежать діючі норми і принципи міждержавного права. Головним слід вважати принцип рівної безпеки.

Стосовно до інформаційної сфери підприємств та організацій сфери економіки, бізнесу та фінансів можна говорити про її трансформацію в принцип адекватної інформованості, який передбачає право на інформаційну безпеку, забезпечення інформаційної безпеки всіх суб'єктів в рівній мірі, врахування інтересів всіх сторін без будь-якої дискримінації, виняток односторонніх переваг, відмова від дій, що завдають шкоди іншому підприємству.

Законодавча база, що визначає перелік відомостей, віднесених до державної таємниці, механізм і порядок її захисту на підприємствах повинні розроблятися, виходячи з принципів та багатосторонніх угод держав, що входять в міжнародну систему інформаційної безпеки. Формування останньої буде, очевидно, справою далекої перспективи, яка ознаменує собою вищий рівень прояву довіри та зацікавленості держав світового співтовариства у забезпеченні виконання на практиці принципу адекватної інформованості. Така система повинна стати підсистемою в системі колективної безпеки [9] підприємств та організацій сфери економіки, бізнесу та фінансів.

1.5. Основні заходи щодо створення і забезпечення функціонування комплексної системи захисту на підприємствах та в організаціях сфери економіки, бізнесу та фінансів

Організаційні заходи є тією основою, яка об'єднує різні заходи захисту в єдину систему.

Вони включають:

– разові (одноразово проводяться і повторюються тільки при повному перегляді прийнятих рішень) заходи;

– заходи, що проводяться при здійсненні або виникненні певних змін у автоматизованій системі (АС) або зовнішньому середовищі (за необхідності);

– необхідні заходи, які проводяться системно та періодично;

– необхідні заходи, які проводяться постійно (безперервно або дискретно у випадкові моменти часу).

До разових заходів відносяться:

– заходи щодо створення нормативно-методологічної бази (розробка концепцій та інших керівних документів) захисту АС;

– заходи, здійснювані при проектуванні, будівництві та обладнанні обчислювальних центрів та інших об’єктів АС (виключення можливості таємного проникнення в приміщення, виключення можливості встановлення прослуховуючої апаратури і т.п.);

– заходи, здійснювані при проектуванні, розробці та введенні в експлуатацію технічних засобів і програмного забезпечення (перевірка та сертифікація використовуваних технічних і програмних засобів, документування тощо);

– проведення спецперевірок застосовуваних в АС засобів обчислювальної техніки і проведення заходів щодо захисту інформації від витоку каналами побічних електромагнітних випромінювань і наведень;

– внесення необхідних змін і доповнень в усі організаційно-розпорядчі документи (положення про підрозділи, функціональні обов’язки посадових осіб, технологічні інструкції користувачів системи і т.п.) з питань забезпечення безпеки ресурсів АС і дій у разі виникнення кризових ситуацій;

– створення підрозділу захисту інформації (комп’ютерної безпеки) і призначення позаштатних відповідальних за ІБ в підрозділах і на технологічних ділянках (здійснюють організацію та контроль за дотриманням всіма категоріями посадових осіб вимог щодо забезпечення безпеки програмно-інформаційних ресурсів автоматизованої системи обробки інформації; розробляють та затверджують їх функціональні обов’язки);

– заходи щодо розробки політики безпеки, визначення порядку призначення, зміни, затвердження і надання конкретним категоріям співробітників (посадовим особам) необхідних повноважень з доступу до ресурсів системи;

– заходи щодо створення системи захисту АС і необхідної інфраструктури (організація обліку, зберігання, використання та знищення документів і носіїв із закритою інформацією, обладнання службових приміщень сейфами (шафами) для зберігання реквізитів доступу, засобами знищення паперових та магнітних носіїв конфіденційної інформації тощо);

– заходи щодо розробки правил розмежування доступом до ресурсів системи (визначення переліку завдань, що вирішуються структурними підрозділами організації з використанням АС, а також використовуються при їх вирішенні режимів обробки і доступу до даних;

– визначення переліків файлів і баз даних, що містять відомості, які становлять комерційну і службову таємницю, а також вимог до рівнів їх захищеності від НСД при передачі, зберіганні та обробці в АС; виявлення найбільш ймовірних загроз для даної АС, виявлення вразливих місць процесів обробки інформації і каналів доступу до неї, оцінка можливого збитку, викликаного порушенням безпеки інформації , розробку адекватних вимог за основними напрямками захисту);

– організація охорони і надійного пропускного режиму;

– визначення порядку проектування, розробки, налагодження, модифікації, придбання, дослідження, прийому в експлуатацію, зберігання та контролю цілісності програмних продуктів, а також порядок поновлення версій використовуваних і встановлення нових системних і прикладних програм на робочих місцях захищеної системи (хто володіє правом дозволу на такі дії; хто здійснює, хто контролює і що при цьому вони повинні робити), визначення порядку обліку, видачі, використання та зберігання знімних магнітних носіїв інформації, які містять еталонні та резервні копії програм і масивів інформації, архівні дані і т.п.;

– визначення переліку необхідних та таких, що регулярно проводяться, превентивних заходів та оперативних дій персоналу щодо забезпечення безперервної роботи і відновлення обчислювального процесу АС в критичних си-

туаціях, що виникають як наслідок НСД, збоїв і відмов засобів обчислювальної техніки, помилок в програмах і діях персоналу, стихійних лих.

До заходів, які проводяться періодично, відносяться:

– розподіл реквізитів розмежування доступу (паролів, ключів шифрування і т.п.);

– аналіз системних журналів (журналів реєстрації), прийняття заходів за виявленими порушеннями правил роботи;

– перегляд правил розмежування доступу користувачів до ресурсів АС організації;

– здійснення аналізу стану та оцінки ефективності заходів і застосовуваних засобів захисту та розробка необхідних заходів щодо вдосконалення (перегляду складу і побудови) системи захисту.

До заходів, які проводяться за потребою, відносяться:

– заходи, здійснювані при кадрових змінах у складі персоналу системи;

– заходи, здійснювані при ремонті і модифікаціях обладнання та програмного забезпечення (санкціонування, розгляд і затвердження змін, перевірка їх на задоволення вимогам захисту, документальне відображення змін і т.п.);

– перевірка нового обладнання, призначеного для обробки закритої інформації, на наявність спеціально впроваджених закладних пристроїв, інструментальний контроль технічних засобів на наявність побічних електромагнітні випромінювання і наведень;

– обладнання систем інформатизації пристроями захисту від збоїв електроживлення та перешкод у лініях зв’язку;

– заходи щодо добору і розстановки кадрів (перевірка прийнятих на роботу, навчання правилам роботи з інформацією, ознайомлення з заходами відповідальності за порушення правил захисту, навчання, створення умов, за яких персоналу було б невигідно порушувати свої обов’язки і т.д.);

– оформлення юридичних документів (договорів, наказів і розпоряджень керівництва організації) з питань регламентації відносин з користувачами (клієнтами) і третьою стороною (арбітражем, Третейський судом) про правила вирішення спорів, пов'язаних з інформаційним обміном;

– оновлення технічних і програмних засобів захисту від НСД до інформації у відповідність з мінливою оперативною обстановкою.

Заходи, які проводяться постійно, включають:

– заходи щодо забезпечення достатнього рівня фізичного захисту всіх компонентів АС (протипожежна охорона, охорона приміщень, пропускний режим, забезпечення збереження і фізичної цілісності засобів обчислювальної техніки, носіїв інформації та т.п.);

– заходи щодо безперервної підтримки функціонування та управління (адміністрування) використовуваними засобами захисту;

– організацію явного і прихованого контролю за роботою користувачів і персоналу системи;

– контроль за реалізацією обраних заходів захисту в процесі проектування, розробки, введення в лад, функціонування, обслуговування та ремонту АС;

– постійно (силами служби безпеки) і періодично (із залученням сторонніх фахівців) здійснюваний аналіз стану і оцінка ефективності заходів і застосовуваних засобів захисту [6].

1.6. Загрози процесам аутентифікації у інформаційних системах фінансових установ та підприємств

Як вище було зазначено, основним моментом в управлінні безпекою інформаційної системи фінансової установи або підприємства є особиста відповідальність кожного користувача. Це досягається з допомогою використання механізмів, які закріплюють таку відповідальність. Кожному користувачеві присвоюється умовне ім'я, унікальне в даній системі, а відповідно до

цього імені встановлюється пароль, який користувач повинен зберігати в секреті і пред'являти системі в якості доказу того, що він саме той, за кого видає себе. Таким чином, в управлінні безпекою інформаційної системи (ІС) і її інформаційними ресурсами виділяються два механізму:

1) ідентифікація, яка виражається через відповідне умовне ім'я;

2) аутентифікація, яка виражається через пред'явлення пароля.

Після аутентифікації, доступ до ресурсів системи дозволяється користувачеві у відповідності до політики доступу, впровадженої в ІС, і правами, обумовленими адміністратором на етапі авторизації.

Одночасно з механізмами аутентифікації в ІС мусять бути впроваджені механізми фіксації авторства, які повинні забезпечити неможливість відмови користувача від своїх дій, що забезпечується з допомогою моніторингу і аудиту. У плані розслідування комп'ютерних інцидентів, дані механізми досить надійні і є інструментом аналізу минулих подій. Слід відзначити, що вони *не володіють* властивістю доказовості, тобто їх не можна застосовувати при доказі авторства. Це пов'язано, в перший чергу, з тим, що система захисту є комплексним і складним конгломератом інформаційних технологій, які інтегровані в саму ІС. Для використання даних аудиту в доказі авторства необхідно довести, що сама ІС захищена, що є складним і трудомістким процесом. Крім того, передбачається, що дані аудиту є на 100% вірними, а це, в свою чергу, означає доказ того, що сама ІС захищена на 100%. З теоретичної точки зору створення подібних ІС можливо.

Т.ч., успішність дій по організації захисту інформації має в якості базового стрижня аутентифікацію.

Вимоги до безпеки і механізмам превентивного захисту в сфері інформаційних технологій повинні бути адекватні потенційним загрозам з боку порушника. Дане твердження вірне також і для механізмів аутентифікації. Це означає, що при проектуванні, розробці і впровадженні механізмів аутентифікації необхідно приймати до уваги можливі типи атак, як на протоколи аутентифікації, так і на механізми їх реалізації.

Можливі загрози протоколам аутентифікації можна об’єднати в групи, які приведені нижче.

Пасивне спостереження – є сьогодні однією з самих поширених загроз. Це обумовлено, по-перше, відносною простотою реалізації, а по-друге, складністю виявлення з боку системи безпеки ІВ. У випадку використання криптографічних протоколів аутентифікації атака *не є дієвою*, але вона може застосовуватися спільно з іншими засобами нападу для отримання максимально можливої кількості інформації, як про учасників, так і про конкретний протокол.

Шифрування повідомлень протоколу дозволяє забезпечити їх конфіденційність і робить марними дії зловмисника, якщо ключі, використовувані сторонами, *не були скомпрометовані*.

Вплив на обмін інформацією. Це наступна по складності група загроз аутентифікації. Виражається в тому, що зловмисник перехоплює інформацію, видозмінює її і відсилає одержувачу. У підсумку одержувач упевнений, що він аутентифікувався з законним учасником протоколу, а на ділі – зі зловмисником. Наслідки подібного типу атак можуть бути катастрофічними для введеного в оману учасника, так як в перший чергу порушується цілісність інформації, яка передається. Для додатків, де цілісність є головною вимогою системи безпеки, порушення її (і переданих повідомлень) створює відповідний ризик в вигляді прямих втрат. Саме виходячи з даних міркувань, в інформаційних системах підприємств сфери економіки, бізнесу та фінансів забезпечення цілісності повідомлень є пріоритетним.

Зміна структури протоколу. Даний клас зловживань досить є специфічним і з’явився в результаті аналізу криптографічних протоколів аутентифікації, оскільки атаки перших двох вище розглянутих класів можуть виявитися безрезультатними. Суть даних атак складається в тому, що зловмисник видозмінює структуру протоколів, після чого законні учасники в процесі аутентифікації *не можуть закінчити протокол*.

Наслідки можуть бути самими різноманітними – від простої відмови в обслуговуванні, до отримання порушником доступу до ресурсів ІС.

Видозміна механізмів прийняття рішень. Даний клас атак *не є прямою атакою на протокол*, але використовується досить часто. Він полягає у видозміні механізмів прийняття рішень, таких, як програми перевірки підпису, прийнятті рішень щодо автентичності і т.д. Особливо привабливі в випадку, коли готується атака на конкретного учасника ІС. Виявлення подібного роду зловживань можливе тільки при реалізації самозахисту механізмів забезпечення безпеки і наявності довірчої комп'ютерної бази.

Піддамо аналізу найбільш поширені загрози процесам аутентифікації.

Криптоаналіз. Криптоаналіз є самим відомим методом атаки на будь-які моделі захисту, що використовують криптографічні операції. Але зі становленням криптографії, як окремої галузі науки, інформаційна індустрія прийшла до рішень, які зводять до мінімуму зусилля криптоаналітика.

Відомі атаки на криптографічні протоколи без компрометації криптоалгоритму. На практиці стратегія криптоаналітика полягає в аналізі та розробці атаки на протокол і тільки у випадку невдачі – в атаці криптоалгоритму, що, як правило, вимагає значних обчислювальних ресурсів і інвестицій. Сьогодні більшість користувачів, що використовують криптографію для захисту своєї інформації, вибирають стандартні криптоалгоритми, що пройшли апробацію, та які робить атаку методом застосовування механізмів криптоаналізу практично неможливою.

Перехоплення обмінної інформації. Перехоплення повідомлень -0 це несанкціоноване читання інформації. При застосуванні криптографічних методів захисту для побудови протоколів аутентифікації порушник *не зможе* скористатися перехопленою інформацією, якщо йому недоступні відповідні ключі.

Повтор повідомлень. Повтор повідомлень – це повторна передача раніше зареєстрованих повідомлень. Часто виникає необхідність, щоб одержувач був упевнений в тому, що моменти формування, передачі і прийому повідом-

лення дуже близькі один до одного. Це означає, що відправник в момент прийому повідомлення одержувачем знаходиться на іншому кінці каналу зв'язку. Якщо одержувач *не може* в цьому переконатися, його легко ввести в оману, що найчастіше призводить до серйозним наслідків.

Практично дана атака реалізується наступним чином: відправник формує і передає повідомлення, а порушник перехоплює його в каналі зв'язку і затримує до часу, який обирає по своєму розсуду. Прийом застарілого повідомлення в момент, вибраний порушником, може бути непотрібним або навіть представляти небезпеку для одержувача або ІС. Інший спосіб реалізації атаки – перехоплення, а потім – повтор повідомлення. У підсумку одержувач приходить до висновку, що воно відправлено законним відправником.

Якщо при формуванні повідомлення відправник застосовує захищену позначку часу, цього достатньо, щоб виключити можливість затримок, але недостатньо, щоб захиститися від другої небезпеки – отримання повідомлення, створеного дуже давно.

Практично зазначене може бути реалізовано наступним чином. Відправник або порушник під його ім'ям формує повідомлення з майбутньою відміткою часу і поміщає його в електронну пошту з інструкцією передати у вказаний час. Відправник (порушник) має можливість підготувати цілу серію таких повідомлень, які будуть надходити одержувачу в певні моменти часу, створюючи ефект авторського присутності.

Маскарад. Це спроба видати себе за іншого в цілях отримання несанкціонованого доступу до інформаційних ресурсів або розширення повноважень. Якщо строго розглядати дану загрозу, то на ділі вона означає порушення стану аутентифікації.

Дезорганізація. Це незаконна зміна адресної частини переданої інформації. Слід відзначити, що недооцінка даної загрози може привести до порушення цілісності технологічних процесів обробки даних і, відповідно, до значних матеріальних втрат. Дезорганізація може привести до того, що хтось або всі *не зможуть* завершити протокол, тобто *не зможуть* аутентифікува-

тися, а в підсумку *не отримають* доступ до інформаційних ресурсів. Підсумком реалізації даної загрози буде відмова в обслуговуванні.

Маніпуляція. Це незаконна заміна, вставка, видалення або переупорядкування даних в інформаційних потоках. У чимось маніпуляція схожа з дезорганізації. Основна відміна складається в тому, що якщо дезорганізація *не має* чітко сформульованої мети, а наслідки можуть бути непередбачуваними, то при маніпуляції даними передбачається досягнення заздалегідь відомої мети.

Відмова від зобов'язань. Відмова від зобов'язань складається у відмові від раніше прийняти або переданих повідомлень (*взятих на себе зобов'язань*). Дана загроза є самою поширеною в системах електронної торгівлі і банківських інформаційних системах, коли користувач відмовляється від проведених раніше транзакцій.

Розвиток технологій, в особливості поява криптографічних грифів, дозволило вирішити дану проблему. Застосування електронного цифрового підпису дозволяє фіксувати авторство повідомлення і попередити відмови від авторства або прийнятих зобов'язань.

Підкидання ключів. Дана загроза є самою поширеною атакою на протоколи, які засновані на криптографії з відкритими ключами. Атака складається в тому, що зловмисник представляє свій публічний ключ замість публічного ключа легального користувача. У випадку, якщо він підписує повідомлення своїм секретним ключем, одержувач вирішить, що він отримав підписане повідомлення від законного учасника процесу обміну даними. Ця атака є особливо небезпечною для фінансово-банківських систем зважаючи на те, що зловмисник може сформувати повідомлення від імені законного користувача. В підсумку – може бути проведена незаконна транзакція.

Для запобігання можливості подібного роду атак використовується ієрархічна система сертифікації, яка реалізує тристоронні довірчі зв'язки. В результаті в рамках системи виділяються головні, довірені органи, які формують так звані сертифікати публічних ключів користувачів. У результаті сертифікації формується логічний зв'язок між ім'ям користувача (володаря

ключа) і конкретним публічним ключем. Підпис головного уповноваженого доводиться до відома всіх учасників системи обміну: вони можуть довіряти ключу і вірити, що публічний ключ, зазначений в сертифікаті, належить користувачеві, ім'я якого значиться в цьому сертифікаті.

Атака рефлексією з паралельним протоколом. Дана атака полягає в тому, що порушник ініціює зустрічний протокол. Він (зловмисник) посилає ті ж питання, які він отримує. Наприклад, якщо хтось запитував пароль, можна йому ж паралельно адресувати це питання. У випадку отримання відповіді, його можна повернути в якості відповіді, і ця відповідь буде прийнята як вірна.

Головний в центрі. Дана атака полягає в тому, що порушник веде діалог одночасно з кожним з учасників, а вони думають, що працюють безпосередньо самостійно.

Однозначне віднесення конкретної загрози до тієї або іншої групи утруднено, зважаючи на їх складності і різнобічності. Але з упевненістю можна визначити приналежність окремих характеристик загроз до тієї або іншої групи. Більш того, з розвитком інформаційних технологій і теорії аналізу протоколів аутентифікації спостерігається поява видів і різновидів атак, які суміщають в собі дві або більше описаних вище загроз. Це означає, що при розробці протоколів аутентифікації повинні прийматися до уваги їх стійкість по відношенню не тільки до звичайних загроз, але й до їх модифікацій і об'єднання в більш складні, інтегровані загрози.

1.7. Огляд та аналіз поточного стану технологій розпізнавання образів та перспективи їх використання у системах захисту інформації

1.7.1 Передумови до використання біометричної аутентифікації у системах захисту інформації

Аналіз поточного стану технологій та перспектив їх розвитку

На сьогоднішній день в різних галузях науки і техніки відчувається зростання потреб у переробці, аналізі та відображенні візуальної інформації. Як слідує з загальнодоступних літературних джерел, це відноситься і до СЗІ, які функціонують у галузі економіки, бізнесу та фінансів, де одним з найважливіших шляхів їх розвитку є створення пристроїв ідентифікації особи абонента з використанням біометричних даних в цілях захисту інформації від несанкціонованого використання або навмисного спотворення.

Задача відноситься до проблем, які вирішуються у рамках теорії розпізнавання образів. Її місце у загальній схемі функціонування технологічної системи, яка використовує СЗІ та технології прогнозування стану при виникненні в ній інцидентів, показане на рис. 1.1.

Загальноприйняті уявлення про теорію розпізнавання образів розуміють, що задача розпізнавання відноситься до класу задач, які вирішуються у рамках цифрової обробки сигналів. Проте останні наукові теорії вважають, що розпізнавання образів є окремим напрямком у науці. Як зазначається у достатньо чисельних наукових та науково-популярних джерелах [15-22], поняття про теорію розпізнавання образів потребує свого уточнення й далі, і на основі цього, потребує уточнення формальна постановка задачі щодо розпізнавання образів у сфері СЗІ, які використовуються у галузі економіки, бізнесу та фінансів.

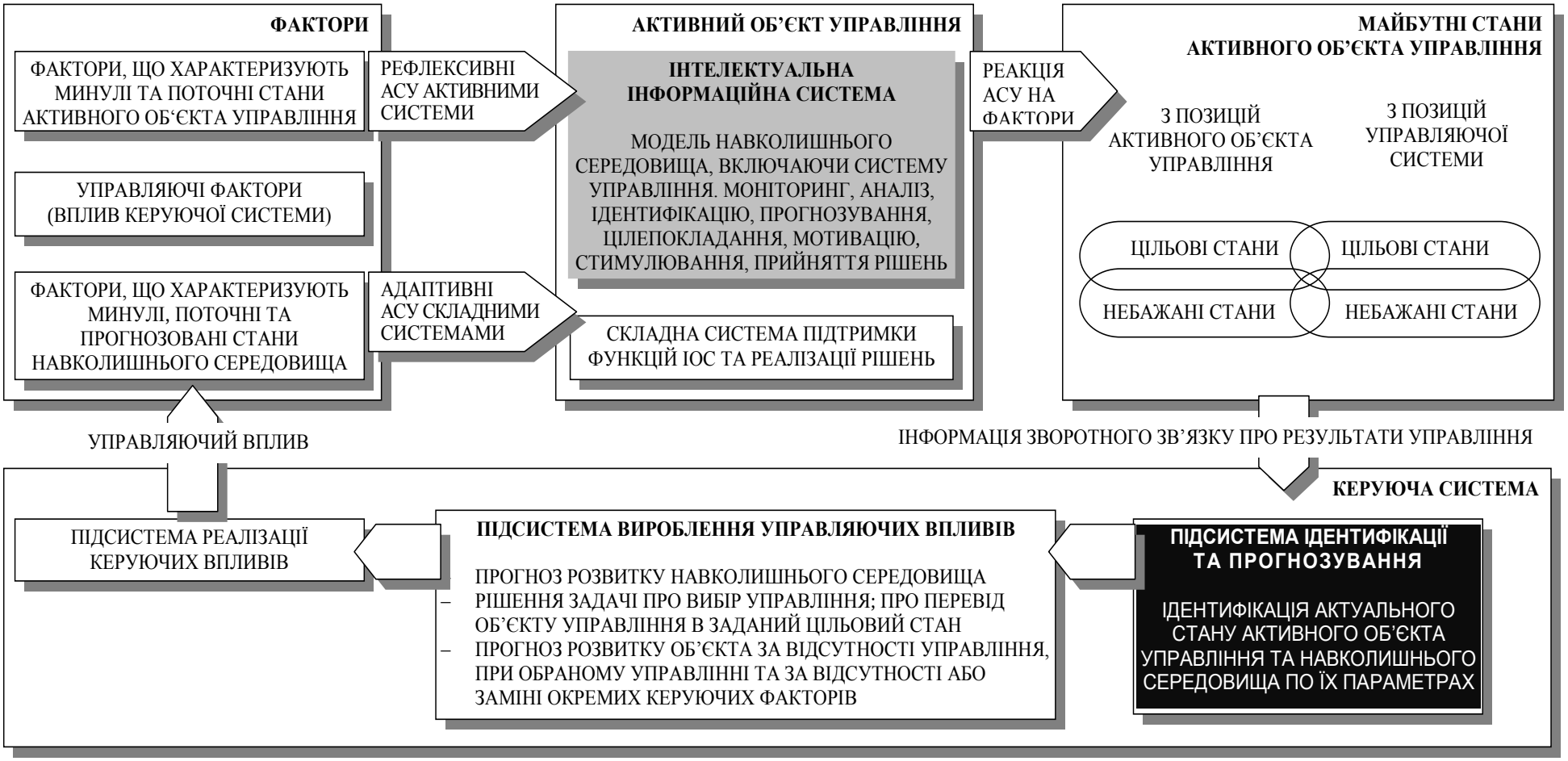


Рис. 1.1. Узагальнена схема функціонування технологічної системи,
яка використовує СЗІ та технології прогнозування стану

На момент проведення досліджень за темою, яка винесена у заголовок НДР, загальний стан біометричних технологій у світі ще не можна визнати задовільним. Скоріше мова може йти про біометрію, як про науково-практичний напрямок, який швидко розвивається та має достатньо велику множину областей дослідження і розробки практичних додатків. Досягнення у ньому необхідних якісних показників, як показав цілий ряд серйозних перевірок, проведених останнім часом, показав недостатню надійність таких систем. Так, наприклад, поліцейське управління міста Тампа, штат Флорида (США), після двох років експлуатації, вивело з експлуатації за марністю програмне забезпечення впізнання осіб, яке працювало разом з камерами зовнішнього спостереження. Передбачалося, що технічне оснащення в комплекті з програмним забезпеченням сканування/упізнання осіб, приєднані до бази правопорушників та дітей, що знаходяться у розшуку, підвищить ефективність роботи поліції. Однак, за два роки система не дала ні єдиного успішного результату. Програмне забезпечення було надано компанією *Identix*, одним з ведучих у США постачальників біометричних технологій розпізнання по зовнішності особи та відбитках пальців.

Відомий звіт японського криптографа Ц. Мацумото, який привів десять прикладів, де він приймав участь з метою компрометації систем ідентифікації користувачів по відбитках пальців. Аналогічне дослідження було проведене у Німеччині одним із комп'ютерних журналів. Висновки були однозначні: біометричні системи для споживчого ринку не досягли того рівня та ефективності, коли їх можна було б розглядати в якості реальної альтернативи традиційним паролям.

Що стосується систем упізнання користувача по відбиткові пальця за допомогою ємнісного сенсора на мишці або клавіатурі, то тут найпоширенішим способом обману є повторне «оживлення» уже наявного відбитка, залишеного зареєстрованим користувачем. Виявилося, що для «реанімації» залишкового відбитка досить просто подихати на сенсор або прикласти до нього тонкий поліетиленовий пакет, наповнений водою. Технологія була вдало випро-

бувана експертами на мишках *ID Mouse* фірми *Siemens*, оснащених ємнісним сенсором *Fingertip* виробництва *Infineon*. Нарешті, «штучний палець», відлитий у парафіновій формі з силікону, дозволив дослідникам здолати всі дактилоскопічні системи, які можна було знайти для тестування.

Систему впізнання осіб по характерним особливостях обличчя *Facevacs-logon* фірми *Cognitec,* групі експертів вдалося ввести в оману, пред'явивши фотографію зареєстрованого користувача. Для обману більш витонченого програмного забезпечення тієї ж фірми, яке аналізувало характерні ознаки живої людини, був успішно застосований екран ноутбука на якому демонструвався відеокліп з записом рухів особи.

Експертна група показала, що більш складно ввести в оману систему для розпізнання по райдужній оболонці ока (використовувалося обладнання *Authenticam BM-ET100* фірми *Panasonic*). При такому способі інфрачервоні датчики реагують не тільки на характерний візерунок зображення райдужки, але й на глибину розташування зіниці. Однак, експерти зробили невеликий отвір на місці зіниці у фотознімку ока, куди під час розпізнання дивилася інша людина. Як результат, системою було прийняте невірне рішення.

Однак, незважаючи на загальну негативну оцінку сучасного стану біометричних систем ідентифікації особистості, в усьому світі спостерігається тенденція до розвитку досліджень та розробок в області біометрії. При цьому однією з основних тенденцій є поступовий перенос пріоритетів з контактних на безконтактні методи біометричного розпізнавання. Причиною цього є підвищення вимог до функціональних можливостей автоматичних систем безпеки, пов'язаних з необхідністю в реальному часі виконувати необхідні дії по встановленню особистості присутніх на контрольованій території людей, причому, досить часто – потай, тобто не тільки безконтактно (дистанційно), але й без спеціального дозволу на використання біометричних ознак з боку персон, які ідентифікуються. Створенню таких біометричних систем нового покоління перешкоджають ряд специфічних проблем, які поки що ще не мають адекватного розв'язку.

Перша група проблем пов’язана з тим, що системи, метою яких є забезпечення безпеки, повинні працювати в умовах природньої поведінки людини, яка не пред’являє спеціального ідентифікатора особа у вигляді виголошення заздалегідь відомих ключових фраз. У цьому випадку ще до розв’язку завдання розпізнавання необхідно вирішити задачу визначення місця розташування та виділення людини в групі з метою вироблення управлінських дій для дистанційно керованих мікрофонів. Втім, це не спрощує саму процедуру розпізнавання особи по голосу в неконтрольованих умовах.

Друга група з існуючих проблем розпізнавання пов’язана з тим, що у для випадку завдання *забезпечення безпеки* (на відміну від *завдання забезпечення контролю доступу*) немає можливості обпертися на співробітництво персони, яка підлягає ідентифікації, навіть на етапі навчання. У таких випадках для навчання використовуються наявні фрагментарні та різнорідні аудіо- та відеоматеріали всілякої якості та походження. Це ще більш ускладнює завдання навчання біометричної системи.

Третя, остання група проблем, пов’язана з тим, що отримані (з урахуванням перерахованих проблем) імовірності правильного розпізнавання та неправильного виявлення заданої персони в природній обстановці тільки по особі або тільки по голосу, виявляються суттєво нижче показників, необхідних для задовільного функціонування систем забезпечення безпеки та, у нашому випадку – СЗІ, а також контролю доступу. Саме з цим пов’язана необхідність комплексування результатів біометричного розпізнавання, отриманого від різних джерел інформації.

Як слідує зі сказаного, з вирішенням зазначених проблем можуть бути зв’язані істотні прориви в області біометричних технологій у найближчі роки.

1.7.2 Визначення цільових завдань СЗІ, які використовують біометричні дані

Узагальнення проблеми обробки візуальної інформації у СЗІ

Завдання розпізнавання образів у СЗІ, згідно до багатьох літературних джерел, включаються у коло задач штучного інтелекту.

У напрямку загальної теорії розпізнавання образів прийнято виділяти *три основних типи завдань*, які ще в 1986 році виділив Т. Павлідіс [15] у рамках проблеми обробки візуальної інформації. З тим пір виділені ним завдання ніким уточнені та дороблені у сенсі класифікації не були. Класифікація завдань по Т. Павлідісу є такою, як це показано на рис. 1.2.

КЛАСИФІКАЦІЯ ЗАВДАНЬ ОБРОБКИ ВІЗУАЛЬНОЇ ІНФОРМАЦІЇ ПО Т. ПАВЛІДІСУ

ОБРОБКА	Обробка зображень, коли і вихідні дані, а також результати обробки представляються в образотворчій формі, тобто у вигляді фотографій, кадрів з відеофільмів та ін.
АНАЛІЗ	Вхідні дані є зображенням, а результат представляється у необразотворчій формі, наприклад у вигляді текстового опису спостережуваної сцени
СИНТЕЗ	На вході є опис (алгоритм побудови) зображення, а на виході з нього будується саме зображення

Рис. 1.2. Класифікація завдань обробки візуальної інформації по Т. Павлідісу

Примітка до рис. 1.1: Під *аналізом* Т. Павлідіс розуміє *інтерпретацію, розпізнавання* або «*розуміння*» зображень [15]. Під *синтезом* Т. Павлідіс розуміє *машинну графіку* [15].

Взаємозв’язок трьох перерахованих типів завдань так, як це зроблено в [16], приведений на рис. 1.3.

Рис. 1.3. Взаємозв’язок напрямків обробки зображень

Як видно з рис. 1.3, *обробка зображень* у СЗІ, пов’язана з перетворенням образотворчої інформації знову в образотворчу форму. Основною метою такого перетворення є, за необхідністю, усунення шумів, спотворень та інших дефектів на зображенні, що веде до поліпшення якості одержуваної візуальної інформації шляхом підвищення контрасту, підкреслення контурів об’єктів та ін. Основні напрямки обробки зображень виділені М. Горським та В. Олександровим у працях [17-19, 23].

Слідуючи логіці, з рис. 1.3 та з [16-19, 23] можна встановити, що *завданням аналізу зображень* у СЗІ є отримання з зображення, поданого на вхід системи, необразотворчого опису.

Як показано в [16], опис образів у СЗІ може бути різних рівнів спільності – від простого зазначення номера або імені класу, до якого належить аналізоване зображення, до докладної текстової характеристики спостережуваної сцени із зазначенням окремих об’єктів та відносин між ними. В останньому випадку мова йде про «розуміння» зображень.

Багато авторів називають аналіз зображень *розпізнаванням*, але у нашому випадку, цей термін має вужче значення, та переважно відноситься до *ідентифікації* окремих об’єктів на зображеннях. Використовувані нами означення щодо понять «розпізнавання» та «ідентифікація», приведені у Додатку А. Там же зазначені типові завдання аналізу зображень.

Стосовно задачі ідентифікації особи абонента інформаційної або іншої мережі з обмеженим доступом, де в цілях захисту інформації від несанкціонованого використання або навмисного спотворення, можуть використовуватися біометричні показники, приведені у Додатку А у вигляді означень та пояснень до них.

Не зважаючи на велику кількість досліджень, включаючи дослідження у СЗІ, створення штучних систем розпізнавання у сенсі ідентифікації конкретної особи залишається складною теоретичною та технічною проблемою. Необхідність у такому розпізнаванні виникає в самих різних областях – від військової справи та систем безпеки до оцифровки всіляких аналогових сигналів. Аналіз численних наукових праць показав, що можна виділити два основних напрямки розпізнаванні образів:

1) вивчення здібностей до розпізнавання, якими володіють живі істоти, пояснення, математичний опис та їх моделювання;

2) розвиток теорії та методів побудови пристроїв, призначених для вирішення окремих завдань в прикладних цілях.

Стосовно задач СЗІ, які вирішуються в дисертаційній роботі, оберемо другий напрям та базуючись на аналізі літературних джерел, визначимо ті методи, які використовуються для автоматичного розпізнавання осіб.

Задача ідентифікації та розпізнавання осіб – це одне з перших практичних завдань, яке стимулювало становлення та розвиток теорії розпізнавання та ідентифікації об’єктів. Згідно до [24], існує дев’ять категорій об’єктів, які відповідають гностичним областям та впливають на прийняття рішень при розпізнаванні та ідентифікації: фізичні об’єкти, якими можна вільно маніпулювати; фізичні об’єкти, якими можна маніпулювати, прикладаючи зусилля або за допомогою проміжних механізмів чи засобів; фізичні стаціонарні об’єкти, якими не можна маніпулювати без зміни їх фізичної сутності; особи; вирази облич; живі істоти; друковані знаки; рукописні зображення; характеристики та розташування джерел світла.

У свою чергу кожна з приведених категорій може бути розділена на менші внутрішні категорії в залежності від прикладної області використання та поставленої мети.

Зосередимося на проблемі підвищення ефективності методів забезпечення спостереженості у технологічних системах спеціального призначення, тобто на задачі розпізнавання осіб. З цією метою нами було використане означення *спостереженості* так, як це передбачено діючими нормативними документами у сфері захисту інформації [20] – див. Додаток А. Поняття, що приведені у Додатку А, у поєднанні з керованістю, становлять *предмет спостереженості*.

Далі будемо використовувати той факт, що якщо існують вимоги щодо контролю за діями користувачів або легальністю доступу і за спроможністю комплексу засобів захисту виконувати свої функції, то відповідні функції будемо відносити до *критеріїв спостереженості*.

Інтерес до процедур, які лежать в основі процесу розпізнавання конкретних осіб, завжди був значним, особливо у зв’язку із зростаючими практичними потребами які на сьогоднішній день виникають в охоронних системах, у системах верифікації, в криміналістичній експертизі і т.д. Незважаючи на ясність того факту, що людина добре ідентифікує обличчя людей, зовсім не очевидно, як навчити ЕОМ проводити цю процедуру, в тому числі – як декодувати та зберігати цифрові зображення осіб. Ще менш ясними є оцінки схожості осіб, включаючи їх комплексну обробку. Як показано в [24], можна виділити такі *напрямки досліджень проблеми розпізнавання осіб*:

– нейропсихологічні моделі;

– нейрофізіологічні моделі;

– інформаційно-процесуальні моделі;

– комп’ютерні моделі розпізнавання.

Проблема розпізнавання осіб у зазначених напрямках розглядалася ще на ранніх стадіях становлення комп’ютерного зору. З того часу ряд компаній протягом більше 40 років активно розробляють автоматизовані, а зараз і ав-

томатичні системи розпізнавання людських облич. До них можна віднести Smith&Wesson (система ASID – *Automated Suspect Identification System*), ImageWare (система *FaceID*), Imagis, Epic Solutions, Spillman, Miros (система *Trueface*), Vissage Technology (система *Vissage Gallery*), Visionics (система *FaceIt*) та ін. Втім, не зважаючи на той період часу, протягом якого ведуться дослідження, у [21] відзначено, що ефективність системи розпізнавання знаходиться на не досить належному рівні і технології, які її забезпечують, ще потребують істотних удосконалень. Так, автори [21] – K. Bonsor та R. Johns?-on, – на основі збору та обробки великої кількості статистичних даних та з посиланнями на *Electronic Privacy Information Center*, показали, що максимальна ступінь розпізнавання у найкращій системі, яка використовується для розпізнавання облич у Бостонському аеропорту у реальному масштабі часу, досягає 61,4%. *Саме цю цифру оберемо у якості опорної при порівнянні ефективності методів забезпечення спостереженості у технологічних системах спеціального призначення*. Крім того, основну увагу будемо приділяти технологіям розпізнавання осіб в автоматичному режимі без врахування режимів автоматичного пошуку та розпізнавання осіб в графічних файлах і відеопотоці. Така постановка задачі звужує сфери застосування методів спостереженості, які розробляються, конкретизуючи їх на системах доступу до технологічних мереж спеціального, критичного та іншого використання, враховуючи інші сфери людської діяльності, що пов’язані з ідентифікацією, авторизацією та аутентифікацією, поняття про які приведені у Додатку А.

Зазначимо, що більшість понять, які приведені у Додатку А, мають декілька значень. У роботі нами використовуються лише ті (за виключенням поняття «Авторизація»), які стосуються СЗІ.

Формальна постановка завдання

Визначимо формальні цільові завдання, які вирішуються при дослідженні.

Першим цільовим завданням є *забезпечення доступності*, яке припускає, що користувач або будь яка особа, яка може отримати доступ до захищеної інформаційної або будь-якої іншої системи, включаючи ТССП, де циркулюють певні дані, володіє відповідними правами та може використовувати ресурс відповідно до правил, встановлених політикою безпеки. Ця задача спрямована на запобігання навмисних або ненавмисних загроз неавторизованого видалення даних або необґрунтованої відмови в доступі до послуги, спроб використання системи та даних в недозволених цілях. Т.ч., удосконалення рішення та технологій забезпечення доступності до захищеної інформаційної або будь-якої іншої системи, є одним з пріоритетних та актуальних завдань для СЗІ у сенсі їх функціонування у складі ТССП.

Другим завданням передбачається *забезпечення цілісності* захищеної інформаційної системи та даних. Це завдання, як правило, розглядається в двох аспектах. По-перше, це цілісність даних, яка означає, що дані не можуть бути модифіковані неавторизованим користувачем, особою або процесом під час їх зберігання, передачі та обробки. По-друге, цілісність полягає в тому, що жоден компонент системи не може бути видалений, модифікований або доданий тими ж неавторизованими користувачем, особою або процесом.

Стосовно приведених визначень та враховуючи тематику дослідження, актуальним завданням у зазначеному сенсі, є авторизація користувачів та осіб, які можуть бути задіяні або залучені до процесів обробки конфіденційної інформації у ТССП. У рамках НДР питання видалення, модифікації та додавання інформації у захищеній інформаційний системі (включаючи ТССП), не розглядаються.

Третє завдання – *забезпечення конфіденційності* даних та системної інформації. Відповідно до нього передбачається, що інформація не може бути

отримана неавторизованим користувачем під час її зберігання, обробки та передачі.

Як правило та згідно до ISO/IEC 15408, у ТССП завдання вирішується програмними засобами забезпечення доступу до інформаційних ресурсів. Втім, вже на перших кроках можна було б посилити систему захисту, передбачаючи певні організаційні та технічні заходи про які мова йтиметься далі: тут лише виділимо необхідність удосконалення рішень щодо третього з основних цільових завдань систем захисту інформації у ТССП. Виходячи з цього, актуальним завданням у рамках вирішуваної проблеми, як і у попередньому випадку, є автоматична або автоматизована авторизація користувачів та осіб, які мають доступ до ресурсів, які захищаються.

Забезпечення спостереженості є четвертим з цільових завдань. Воно спрямоване на забезпечення можливості інформаційної системи фіксувати *будь-яку діяльність* користувачів та процесів у ТССП, використання пасивних об’єктів, встановлювати ідентифікатори причетних до подій користувачів і процесів з метою запобігання порушенням безпеки та забезпечення відповідальності користувачів за виконані дії.

Саме приведене визначення у найбільш повній мірі відповідає темі дисертаційної роботи, так як передбачає автоматичну фіксацію користувачів інформаційної (як правило – захищеної) системи ТССП, їх діяльність та інші ідентифікатори щодо причетності окремих персон до процесів порушенням безпеки та забезпечення їх відповідальності за виконані дії.

Цільовим завданням, яке завершує перелік, є *забезпечення гарантій* – тобто сукупності вимог, які складають деяку шкалу оцінки для визначення ступеня впевненості в тому, що:

– функціональні вимоги щодо інформаційної безпеки у ТССП дійсно сформульовані та коректно реалізовані;

– вжиті заходи захисту забезпечують адекватний захист інформаційних систем, що функціонують у складі ТССП;

– забезпечена достатня стійкість від навмисного проникнення та використання обхідних шляхів, включаючи фізичний доступ та надійну ідентифіка-

цію користувачів ТССП, об’єктів та процесів.

З позицій інформаційної безпеки та виконання зазначених формальних цільових завдань, саме *аутентифікація* є частиною процедури надання доступу для роботи в інформаційній системі, наступною після ідентифікації та такою, що передує авторизації. Відомості про механізми роботи СЗІ, які базуються на використанні технологій аутентифікації, поняття та відомості про біометричну аутентифікацію, основні етапи проектування системи біометричної аутентифікації з використанням технологій розпізнавання образів, приведені у Додатку Б.

У сукупності удосконалення та підвищення ефективності методів та технологій, які забезпечують процедуру аутентифікації, є смислом дисертаційної роботи.

Розробка загальної схеми дослідження

При постановці завдань розпізнавання (включаючи всі етапи НДР) будемо користуватися математичною мовою, намагаючись, на відміну від теорії штучних нейронних мереж, де основою є отримання результату шляхом експерименту, замінити експеримент логічними міркуваннями та математичними доказами. У цьому випадку для нас класичною постановкою задачі розпізнавання образів у системах забезпечення спостереженості є виконання наступних етапів:

– встановлення множини об’єктів дослідження;

– проведення дослідження щодо належності множини об’єктів до певної класифікаційної структури з метою визначення множини методів їх обробки;

– огляд визначеної множини методів обробки, її аналіз, вибір ефективного методу розробки або удосконалення алгоритмів (методів або методик) обробки відповідно до поставленої мети;

– віднесення розробленого (удосконаленого) алгоритму (методу або методики) до множини (класу) наявних способів доступу до ТССП з метою співставлення та аналізу отриманих результатів.

Виходячи зі сказаного, можна зробити логічний висновок про наступне.

В задачах розпізнавання, ідентифікації та аутентифікації біометричних даних, а саме – образів конкретних осіб, – які тісно зв'язані з процесами забезпечення спостереженості, повинні розглядатися монохромні зображення, що дасть можливість розглядати зображення, як функцію на площині. Якщо розглядати точкову множину на площині T, де функція $f(x,y)$ виражає в кожній точці зображення його характеристику – яскравість, прозорість, оптичну щільність, – то така функція є формальним записом зображення. Множина всіх можливих функцій $f(x,y)$ на площині T – є модель множини всіх зображень x. Вводячи поняття подібності між образами, у необхідних випадках ми зможемо формулювати відповідні задачі розпізнавання. Конкретний вид таких постановок буде залежати від кожного з наступних етапів при розпізнаванні в відповідності з вибраними в подальшому підходами.

Вирішення зазначеної формальної задачі, як результат роботи, повинно підвищити ефективність спостереженості у технологічних системах спеціального призначення, яка може полягати у забезпеченні тих параметрів, які зазначені далі у відповідних підрозділах.

Як проміжний висновок зазначимо, що здійснення цілей розпізнавання може бути досягнуто до моменту завершення процесу розпізнавання. Ступінь досягнення цілей розпізнавання буде характеризувати ефективність реалізації процесу розпізнавання. При цьому чим вищим буде ступінь досягнення цілей розпізнавання при рівності витрат на реалізацію процесів розпізнавання, тим вищою буде його ефективність.

Т.ч., *загальною схемою теоретичних досліджень* є: знаходження деякої функції, яка відображає множину образів (зображень) у множину, елементами якої є класи образів. Процес визначення такої функції пов'язаний з дослідженням наступних теоретичних питань:

1. Теоретичне обґрунтування процесів попередньої обробки, пов'язаних з тим, що задане зображення $f(x)$ необхідно перетворити в одне або кілька

нових зображень $f_1(x,y)...f_n(x,y)$ за допомогою деякого набору або послідовності певних операцій з метою приведення його до встановлених вихідних норм, тобто визначити процедури перетворень кольорового зображення в чорно-біле, масштабування, видалення шумів і т.д.

2. Вибір механізму виділення ознак, який повинен полягати в тому, що функції $f_i(x,y)$ зазнають функціональних перетворень $F_1...F_m$, на основі яких визначаються ознаки зображення і, т.ч., у результаті цього зображення повинне бути представлене у вигляді масивів дійсних чисел, готових до подальшої обробки.

3. Класифікація отриманих результатів, тобто вибір механізму, який дозволить установлені ознаки вихідного зображення $f(x,y)$ зіставити з базою даних зображень.

З врахуванням сказаного, *загальною схемою практичних досліджень* є:

1. Вибір цифрового зображення з заданими параметрами, яке отримане за допомогою спеціальної інфрачервоної фотокамери або WEB-камери з додатковими спеціальними датчиками;

2. Попередня обробка: видалення шумів, яркісна та контрастна корекція, сегментація, колірна корекція – у нашому випадку, це отримання напівтонового зображення та, за необхідністю, його перетворення у чорно-біле зображення;

3. Виявлення локальних ознак серед множини глобальних ознак – розпізнавання;

4. Розуміння або інтерпретація та оцінка (класифікація) об’єкта спостереження.

1.7.3. Огляд та вибір інформативних ознак зображень для розв'язку задачі біометричної ідентифікації особи

Вибір предмета та технології розпізнавання

Складна структура біометричних показників людини не дозволяє ефективно вирішувати завдання аналізу даних по спектральних ознаках безпосередньо так, як це показано, наприклад, [25-27]. Спектральні портрети окремих об'єктів, які можуть бути використані в якості предмета ідентифікації та аутентифікації, як правило, не є стаціонарними, тому що залежать від багатьох факторів, включаючи емоційний стан людини, температурні умови, маскуючі ознаки, положення об'єкта і т.д. Найбільш стаціонарними ідетифікаторами окремої особи можуть бути її термограми, які не змінюються у часі, від впливу зовнішнього середовища, від віку людини та ін. На основі аналізу термограм системи доступу мають можливість розрізняти навіть близнюків, що до теперішнього часу не вдавалося жодній з систем, включаючи системи аналізу ДНК. Втім, щоб підвищити достовірність щодо прийнятя рішень, необхідно використати апріорну інформацію про геометрію зйомки, з одного боку, і контекстну інформацію самих зображень – з іншого.

Згідно до [25], контекстна інформація спостережень виражається у вигляді просторової організації елементів, меж та самих об'єктів. Знання контексту завдання, тобто обмежень, що накладаються на взаємні зв'язки між компонентами зображення, підвищує ефективність вирішальних правил.

Найпростішою формою контекстної інформації для пікселя зображення є околиця цього пікселя. У зв'язку з цим, в [28] доведене твердження про те, що об'єктне вирішальне правило, коли береться фрагмент цілком, ефективніше піксельного вирішального правила.

Іншою формою контекстної інформації є поняття про *контур*. Таке поняття є функціоналом набору пікселів фрагмента. Перевага знаходження контурних ознак полягає в потенційних можливостях агрегації контекстної ін-

формації з певними властивостями інваріантності під конкретне завдання розпізнавання образів з наступною ідентифікацією та аутентифікацією за встановленими правилами.

На жаль, не існує загальноприйнятої теорії синтезу контурних ознак, що забезпечують, наприклад, мінімум середніх помилок розпізнавання. У зв'язку з цим контурні ознаки поки синтезуються окремо для кожного типового випадку, а якість їх перевіряється емпірично для конкретного завдання класифікації. У зв'язку з цим, виправданим може бути узагальнений підхід, який має на увазі синтез великої кількості контурних ознак з наступним дослідженням усіх підмножин створеної системи на інформативність.

Незважаючи на повсюдну присутність усіляких контурів особи на зображеннях та їх важливість для систем біометричної ідентифікації, формального підходу до їхнього опису та строгого визначення нами не знайдене. Методи розрізнення контурів, як і методи виявлення контурних ознак, розробляються окремо для кожного конкретного випадку.

В [29] під поняттям «*контурна структура*» у контексті знаходження та виділення деякої текстури, розуміється «просторова організація елементів у межах деякої ділянки поверхні». Там же пояснюється, що ця організація обумовлена певним статистичним розподілом інтенсивності сірих тонів або тонів різного кольору. Ділянка вважається *контуром*, якщо кількість відмічуваних на ньому перепадів інтенсивності або змін кольору є досить великою. В [30] під таким же поняттям мається на увазі «деяким чином організована ділянка поверхні». Контур в [31], це «матриця або фрагмент просторових властивостей ділянок зображень (в [31] – земної поверхні) з однорідними статистичними характеристиками».

Виходячи зі сказаного, можна узагальнити поняття про контури, згрупувавши їх у такий спосіб [29]:

– контури по походженню:

- штучні: графічні знаки та візерунки, розташовані на нейтральному полі;

- природні: топографічні зображення на картах, фотографії людей, рентгенівські знімки, термограми і т.д.;

– контури за структурою:

- контури, що складаються з геометрично правильних повторюваних елементів;
- стохастичні контури, сформовані перетворенням послідовності корельованих випадкових чисел відповідно до певних розмірів елементів текстури зображення: дрібнозернисті та грубозернисті;

– контури, сформовані за формою елементів виділюваної текстури.

З приведених визначень випливає, що контур, це деяка ділянка зображення, але не будь-яка, а тільки та, яка має однорідні статистичні характеристики. Отже, контур можна описати деякими ознаками. Під такими ознаками розуміють характерні властивості, загальні для всіх контурів даного класу [29], тобто, наприклад, для класу, який умовно назвемо «клас чорно-білих фотографій».

Ознаки контурів відіграють вирішальну роль для їхньої класифікації, а також при поділі зображень на окремі області, що є важливим положенням для використання контурів у системах ідентифікації. З цією метою проведемо аналіз та складемо систему ознак для виділення контурів відповідно до раніше поставленого нами формального завдання.

Аналіз систем контурних ознак

Перед тем як розпочати процедуру розпізнавання контуру, необхідно визначити розмір ковзного вікна, за допомогою якого він буде виділятися. Вибір розмірів вікна обумовлений тим, що контур визначається околицею точки зображення. Від розміру ковзного вікна $(2W+1)(2W+1)$ залежить, які властивості об’єктів характеризують обчислювальны ознаки контурів, а також їх масштаб. Так, у більшому вікні відбиваються властивості текстурної однорідності більших об’єктів. При цьому вплив окремих пікселів вікна на

величину оцінки знижується, просторове розділення кінцевої класифікації помітно погіршується [32]. З іншого боку, у занадто малому вікні може виявитися недостатньо статистичної інформації для адекватного опису властивостей контуру, а також інших об’єктів [33].

У [25, 29] дослідження впливу розміру вікна на правильну інтерпретацію чисельних значень контурних ознак показало, що у вікнах розміром 3×3 або 5×5 пікселів статистичні контурні виміри більше діють як детектори перепадів яскравості, а не як вимірники контурних ознак, хоча при цьому скорочується час обчислень (див. [31]). Занадто великі розміри вікон можуть спотворити результати через вплив країв окремих структур і самих контурів (границь зображень), тобто у вікно можуть потрапити контури інших об’єктів та контури самого об’єкту, які на момент виділення не є предметом розпізнавання. Однак велике вікно дозволяє досягтися високої статистичної ймовірності.

Як виявилося, вікна 20×20 пікселів найбільш ефективні для попередньої загальної текстурної обробки [31]. Там же говориться, що при зміні розмірів вікна від 80×80 до 20×20 пікселів чисельні значення контурних ознак змінюються на 5...10%. Подальша зміна розміру вікна привела до значного спотворення необхідних ознак.

Визначившись з розміром вікна, можна приступити до формування системи ознак. В [29] показано, що ознак існує досить багато і їх можна розділити на групи:

– ознаки, засновані на вимірі просторових частот;

– ознаки, засновані на статистичних характеристиках рівнів інтенсивності елементів розкладання;

– ознаки, засновані на описі структурних елементів;

Надалі в роботі будемо дотримуватися наведеного поділу ознак.

Проведемо аналіз ознак, які можемо використати для виділення контурів і, базуючись на отриманих результатах, отримаємо вихідні дані для розробки системи ідентифікації особи для СЗІ.

Ознаки, засновані на вимірі просторових частот

Першою ознакою, яка може служити для виділення контурів [25, 29], та яка базується на вимірі просторових частот, є автокореляційна функція, приведена у [34]:

$$A(\xi,\eta;j,k)=\frac{\sum_{m=j-W}^{j+W}\sum_{n=k-W}^{k+W} f(m,n)\,f(m-\xi,n-\eta)}{\sum_{m=j-W}^{j+W}\sum_{n=k-W}^{k+W}\left[f(m,n)\right]^2}.$$

Як показано там же, вона обчислюється у вікні розміром $(2W+1)\times$ $\times(2W+1)$ для кожної точки зображення (j,k) з урахуванням зсуву вікна на $(\xi,n)=0;\pm1;\pm2;\ldots$, де $f(m,n)$ – яскравість пікселя в точці (m,n).

При фіксованому цілочисельному зрушенні (ξ,η) більші значення $A(\xi,\eta,j,k)$ відповідають області грубозернистої текстури, тобто розмір зерна пропорційний ширині автокореляційної функції, яка по визначенню є другим моментом:

$$T(j,k)=\sum_{\xi=-T}^{T}\sum_{\eta=-T}^{T}\xi^2\eta^2 A(\xi,\eta;j,k). \qquad (1.1)$$

Як видно, співвідношення (1.1) може служити ознакою, яка характеризує зернистість зображення.

У якості другої ознаки, яка базується на вимірі просторових частот [25], можна використовувати систему ознак, засновану на аналізі спектра Фур'є для конкретного зображення $f(x,y)$ [29]:

$$F(u,v)=\int_{-\infty}^{+\infty}\int f(x,y)e^{-2\pi i(ux+vy)}dxdy.$$

Враховуючи, що радіальний розподіл спектра потужності $|F|^2$ є чутливим до зернистості зображення, систему ознак можна скласти зі значень спектра, усереднених у межах кілець, центри яких перебувають на початку ко-

ординат, тобто $\Phi_r = \int_0^{2\pi} \left|F\left(r,\theta\right)\right|^2 d\theta$, де r – радіус. Кутовий розподіл спектра потужності є чутливим до орієнтації окремих векторів контуру. Контурному зображенню, яке виділяється з об'єкта, що має границі, орієнтовані в якомусь одному напрямку θ, відповідає більша величина спектра, зосереджена поблизу напрямку $\theta \pm \frac{\pi}{2}$. У той же час, для об'єкта, який не має границь чітко спрямованого характеру, відповідає ненаправлений спектр. У цьому випадку ознаки формуються усередненням спектра в межах секторів, які мають вершини на початку координат:

$$\Phi_\theta = \int_0^{\infty} \left|F\left(r,\theta\right)\right|^2 dr. \qquad (1.2)$$

Для зображення, яке може бути представлено в цифровій формі у вигляді матриці $n \times n$ елементів, безперервне перетворення Фур'є заміняють його дискретним аналогом:

$$F\left(u,v\right) = \frac{1}{n^2} \sum_{k=0}^{n-1} \sum_{j=0}^{n-1} f\left(k,j\right) e^{-2\pi i(ku+lv)}, \quad 0 \le \left(u,v\right) \le n-1. \qquad (1.3)$$

Тоді система ознак прийме вигляд:

$$\begin{aligned} \Phi_{r_1,r_2} &= \sum \left|F\left(u,v\right)\right|^2 \left| \begin{array}{l} r_1^2 \le u^2 + v^2 \le r_2^2 \\ 0 \le \left(u,v\right) \le n-1. \end{array} \right. \\ \Phi_{\theta_1,\theta_2} &= \sum \left|F\left(u,v\right)\right|^2 \left| \begin{array}{l} \theta \le arctg\left(\frac{u}{v}\right) \le \theta_2; \\ 0 \le \left(u,v\right) \le n-1. \end{array} \right. \end{aligned} \qquad (1.4)$$

Спільне використання ознак (1.3) та (1.4) дозволяє зробити систему чутливою як до розмірів, так і до орієнтації елементів, що утворюють контур. У такій системі ознак використовується не більш чотирьох кілець і чотирьох секторів. Відзначимо, що при здійсненні перетворення (1.2), відповідно до [25, 29], вихідне зображення $f\left(k,j\right)$ розглядається як періодичне, тобто, начебто крайній лівий стовпець матриці вхідного сигналу точно відповідає крайньому правому стовпцю, а верхній рядок – нижньому. Оскільки, як пока-

зали результати моделювання, у дійсності крайні стовпці та рядки відрізняються один від одного, то у вхідному сигналі з'являються стрибкоподібні крайові ефекти. Внаслідок цього виникає ефект неправильної спрямованості, так як в спектрі потужності з'являються високі частоти, що веде до неправильного встановлення ознак контуру.

Для компенсації вище наведеного ефекту, при практичній реалізації процедури розпізнавання контуру, використовують метод придушення впливу апертури, який заснований на дзеркальному відбитті заданого зображення по осях x та y для одержання зображення розміром $2n \times 2n$. У новому зображенні верхні та нижні рядки, а також крайні стовпці збігаються і, т.ч., крайові ефекти не виникають.

Проведені експериментальні дослідження показали, що застосування методу придушення впливу апертури при знаходженні ознак контурів по спектру Фур'є, дозволяє збільшати ймовірність їх правильного виділення в середньому на 6%, що корелюється з результатами з [25, 29]. Втім, це не дає приводу до того, щоб використовувати розглянуту ознаку в системах біометричної ідентифікації у зв'язку з великою обчислювальною складністю та великих витратах машинного часу.

Ознаки, засновані на статистичних характеристиках

У якості ознак, які засновані на статистичних характеристиках зображення, можна використовувати статистичні моменти просторових розподілів. Вони обчислюються як виміри однорідностей по одномірній гістограмі значень сигналів (характеристики 1-го порядку) і по двовимірним гістограмах значень сигналів (характеристики 2-го порядку).

Так, у якості чисельних оцінок контурів по одномірній гістограмі можна використовувати наступні статистичні характеристики [33]:

– k-й початковий момент:

$$T_1^k = n^{-2}\sum_{i=1}^{n}\sum_{j=1}^{n}\left[f(i,j)\right]^2; \qquad (1.5)$$

– ентропію:

$$T_2 = -\sum_{g=0}^{N-1} F(g)\log_{10} F(g); \qquad (1.6)$$

– енергію:

$$T_3 = -\sum_{g=0}^{N-1}\left[F(g)\right]^2; \qquad (1.7)$$

– варіацію:

$$T_4 = -\sum_{g=0}^{N-1}(g-\mu)^2 F(g), \qquad (1.8)$$

де n – розмір ковзного вікна в пікселях; $f(i,j)$ – яскравість пікселя в точці (i,j) ковзного вікна; N – кількість градацій яскравості зображення; $F(g)$ – кількість пікселів з яскравістю g; μ – середнє у вікні $\left(T_{mom1}^1\right)$.

Аналіз показує, що контурні оцінки (1.5)-(1.8), які обчислюються по одномірній гістограмі частот, не враховують взаємного розташування сусідніх пікселів у ковзному вікні та дозволяють оцінювати лише групові властивості пікселів, що входять до складу того або іншого об’єкта на зображенні. Т.ч., можна зробити висновок про те, що дані оцінки ефективні лише для опису контурів з невираженою просторовою регулярністю.

Для формування контурних ознак, які враховують взаємне розташування пікселів усередині ковзного вікна, в [30, 31, 33, 35] приводиться підхід, заснований на використанні *матриці суміжності* (в [31] – *матриця розподілу градієнтів*). Надалі будемо використовувати поняття «матриця суміжності».

Нехай аналізоване зображення є прямокутним та має N_x елементів по горизонталі та N_y елементів по вертикалі. При цьому $G=\{1,2,...,N\}$ – множина N квантованих значень яскравості. Тоді зображення описується функцією значень яскравості з множини G, тобто $f: L_x L_y \to G$, де

$L_x = \{1,2,...,N_x\}$ та $L_y = \{1,2,...,N_y\}$ – горизонтальні та вертикальні просторові області, відповідно. Набір N_x та N_y є набір елементів роздільної здатності в растровому зображенні. Матриця суміжності містить відносні частоти p_{ij} наявності на зображенні сусідніх елементів, які розташовані на відстані d один від одного, з яскравостями i, $j \in G$. Звичайно розрізняють горизонтальні $(\alpha = 0^\circ)$, вертикальні $(\alpha = 90^\circ)$ та поперечно-діагональні ($\alpha = 45^\circ$ та $\alpha = 135^\circ$) пари елементів. Слід зазначити, що ці матриці симетричні, а саме: $P(i,j,d,\alpha) = P(j,i,d,\alpha)$.

На основі обчислених матриць суміжності стає можливим розрахунок безпосередньо чисельних оцінок ряду контурних ознак [33]:

– середнє:

$$T_5 = \mu_i = \mu_j = \sum_{i=0}^{N-1}\left[i \sum_{j=0}^{N-1} P(i,j) \right]; \qquad (1.9)$$

– енергія:

$$T_6 = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1}\left[P(i,j) \right]^2; \qquad (1.10)$$

– варіація:

$$T_7 = \sigma_i^2 = \sum_{i=0}^{N-1}\left[(i-\mu_2)^2 \sum_{j=0}^{N-1} P(i,j) \right]; \qquad (1.11)$$

– однорідність:

$$T_8 = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} P(i,j)/(1+|i-j|), \qquad (1.12)$$

де $P(i,j)$ – частота появи двох пікселів у ковзному вікні з яскравістю i та j під кутом α на відстані d; σ_i – середньоквадратичне відхилення яскравості в ковзному вікні.

Статистичні моменти (1.9)-(1.12) дозволяють формувати контурні ознаки, які враховують взаємне розташування сусідніх пікселів у ковзному вікні і, відповідно, є ефективними для опису контурів з вираженою просторовою ре-

гулярністю.

В [29, 31] приводяться наступні загальні ознаки, що використовуються при розпізнаванні зображень, які можна узагальнити на технологію розпізнавання контурів:

– другий кутовий момент $T_9 = \sum_{i=1}^{N}\sum_{j=1}^{N}\left(\frac{P(i,j)}{M}\right)^2$, де M – загальна кількість пар елементів, які примикають один до одного (наприклад, для $d=1$, $\alpha=0$, $M=2N_y(N_x-1)$). Ознака T_9 є атрибутом однорідності (гомогеності) зображення і для елементів, що примикають один до одного, є мінімальним значенням;

– контраст $T_{10} = \sum_{n=0}^{N-1} n^2 \left[\sum_{i=1}^{N}\sum_{j=1}^{N}\frac{P(i,j)}{M}\right], |i-j|=n$: визначається величиною локальних варіацій яскравості зображення. Зі збільшенням числа локальних варіацій контраст зростає;

– коефіцієнт кореляції $T_{11} = \sigma_x^{-1}\sigma_y^{-1}\sum_{i-1}^{N}\sum_{j=1}^{N}\left[ij\left(\frac{P(i,j)}{M}\right) - m_x m_y\right]$, де m_x, m_y, σ_x, σ_y – середні значення та середньоквадратичні відхилення для $p_x(i) = \sum_{j=1}^{N}\frac{P(i,j)}{M}$ та $p_y(j) = \sum_{i=1}^{N}\frac{P(i,j)}{M}$ відповідно. Ознака T_{11} служить мірою лінійності регресійної залежності яскравості на зображенні;

– дисперсія $T_{12} = \sum_{i=1}^{N}\sum_{j=0}^{N}(i-m)^2\left(\frac{P(i,j)}{M}\right)$: визначає варіації яскравості щодо середнього значення;

– момент зворотної різниці $T_{13} = \sum_{i=1}^{N}\sum_{j=1}^{N}\left[1+(i-j)^2\right]^{-1}\left(\frac{P(i,j)}{M}\right)$: тісно пов’язаний з контрастом та відображає ступінь розкиду елементів матриці градієнтів навколо головної діагоналі. Ця ознака є альтернативою контрасту у випадку виділення крайових структур, оскільки відносно більші різниці в значеннях яскравості вносять мінімальний вклад у кінцевий результат.

– сумарне середнє: $T_{14} = \sum_{n=2}^{2N} n p_+(n)$, де $p_+ = \sum_{i=1}^{N}\sum_{j=1}^{N} \frac{P(i,j)}{M}$ при $i + j = n$, $n = 2,3,...,2N$ – гістограма сум значень яскравості. Ознака T_{14} визначається гістограмою сум значень яскравості $p_+(n)$ по парах елементів зображення, яка безпосередньо пов'язана з матрицею суміжності;

– сумарна дисперсія $T_{15} = \sum_{n=2}^{2N} (n - T_{14})^2 p_+(n)$: служить мірою варіацій яскравості щодо сумарного середнього;

– сумарна ентропія для гістограми сум значень яскравості $T_{16} = \sum_{n=2}^{2N} p_+(n) \log p_+(n)$ визначається класичною мірою статистичної теорії інформації та виражає нерівномірність розподілу яскравісних властивостей елементів зображення;

– етропія $T_{17} = \sum_{i=1}^{N}\sum_{j=1}^{N} \left(\frac{P(i,j)}{M} \right) \log \left(\frac{P(i,j)}{M} \right)$: визначається так само, як і сумарна ентропія, але тільки для матриці суміжності;

– диференціальна дисперсія $T_{18} = \sum_{n=0}^{N-1} \left[n - \sum_{m=0}^{N-1} p_-(m) \right]^2 p_-(n)$, де $|i - j| = m$: виражається через гістограму різниць значень яскравості $p_-(n) = \sum_{i=1}^{N}\sum_{j=1}^{N} \frac{P(i,j)}{M}$ по парах елементів зображення, яка утворюється з матриці суміжності;

– диференційна ентропія $T_{19} = -\sum_{m=0}^{N-1} p_-(n) \log p_-(n)$: розраховується як сумарна ентропія та ентропія для матриці суміжності, але для гістограми різниць значень яскравості;

– інформаційна міра кореляції:

$$T_{20} = T_{17} + \frac{\sum_{i=1}^{N}\sum_{j=1}^{N} P(i,j) \left[\log \sum_{i=1}^{N} p(i,j) \sum_{i=0}^{N} p(i,j) \right]}{\max\{H(X) H(Y)\}},$$

де $H(X)=-\sum_{i=1}^{N}\sum_{j=1}^{N}\left(\frac{P(i,j)}{M}\right)\log\sum_{j=1}^{N}\left(\frac{P(i,j)}{M}\right)$; $H(Y)=-\sum_{j=1}^{N}\sum_{i=1}^{N}\left(\frac{P(i,j)}{M}\right)\log\sum_{i=1}^{N}\left(\frac{P(i,j)}{M}\right)$,

$p(i,j)=\frac{P(i,j)}{M}$;

– інформаційна міра $T_{21}=\left\{1-\mathrm{e}^{-2\left(-\sum_{i=1}^{N}\sum_{j=1}^{N}K(i,j)-T_{17}\right)}\right\}^{0,5}$, де $K(i,j)=\sum_{j=1}^{N}\left(\frac{P(i,j)}{M}\right)\times$

$\times\sum_{i=1}^{N}\left(\frac{P(i,j)}{M}\right)\log\left(\sum_{j=0}^{N}\left(\frac{P(i,j)}{M}\right)\sum_{i=1}^{N}\left(\frac{P(i,j)}{M}\right)\right)$.

Інформаційні міри визначаються співвідношеннями класичної статистичної теорії інформації для елементів матриці суміжності, гістограми сум значень яскравості та гістограми різниць значень яскравості.

– максимальний коефіцієнт кореляції (друге найбільше власне значення Q) $T_{22}=Q^{0,5}$, де $Q=\frac{\sum_{i=1}^{N}\left(\frac{P(i,k)}{M}\right)\left(\frac{P(j,k)}{M}\right)}{\sum_{j=1}^{N}\left(\frac{P(i,k)}{M}\right)\sum_{i=1}^{N}\left(\frac{P(i,k)}{M}\right)}$ – нормована енергія матриці суміжності, що обчислюється по матриці суміжності, рядах з елементів рядків та стовпців цієї матриці, та має властивості, які не проявляються в T_{11} (коефіцієнт кореляції).

Ознаки T_9, T_{16}, T_{17}, T_{19}, T_{20}, T_{22} мають властивості інваріантності при монотонних перетвореннях яскравості. Як свідчать численні літературні джерела, для реальних контурів, перед обчисленням матриці розподілу градієнтів, динамічний діапазон зображень по яскравості доцільно зменшити шляхом відповідної нелінійної обробки (наприклад, еквалізації) до $N=4...16$.

Контурні ознаки також можна виділити з використанням двовимірної гістограми розподілу яскравостей, яка будується в такий спосіб: уводиться двовимірний цілочисельний масив $B(s,r)$ з розмірністю N по кожній координаті. Далі, через $S(*)$ позначається інтенсивність оцифрованого зображен-

ня першого з каналів, які аналізуються, а через $R(*)$ – інтенсивність оцифрованого зображення другого каналу даних. Далі аналізуються яскравості каналу $s \in S$ та каналу $r \in R$. Ці значення округляються до найближчого цілого і здійснюється акумуляція частот усіх пар значень (s,r) у масиві $B(s,r)$ з наступним нормуванням за необхідною шкалою. На підставі цієї двовимірної гістограми розподілу яскравостей можна виділити наступні основні ознаки:

– середнє по першому каналу: $S(*)\,T_{23} = \sum_{-m}^{m}\left[\mu \sum_{-m}^{m} B(\mu,\nu)\right],\ \mu \in S(s,r)$;

– середнє по другому каналу: $R(*)\,T_{24} = \sum_{-m}^{m}\left[\nu \sum_{-m}^{m} B(\mu,\nu)\right],\ \nu \in R(s,r)$.

– ентропія: $T_{25} = -\sum_{-W}^{W}\sum_{-W}^{W} B(\mu,\nu)\ln(\mu,\nu)$.

– енергія: $T_{26} = -\sum_{-W}^{W}\sum_{-W}^{W}\left[B(\mu,\nu)\right]^2$.

– кореляція: $T_{27} = \sum_{-W}^{W}\sum_{-W}^{W}(\mu - T_{23})(\nu - T_{24})B(\mu,\nu)$.

– інформаційна міра: $T_{28} = \sum_{-W}^{W}\sum_{-W}^{W} B(\mu)B(\nu)\ln B(\mu,\nu)$.

Ознаки, що засновані на описі структурних елементів

Як випливає з літературних джерел [29, 36, 37], останнім часом усе більший розвиток отримує структурний підхід до опису контурів. Він заснований на аналізі форми та розмірів елементів, що становлять контур, з наступним обчисленням локальних ознак та аналізом розподілу окремих елементів контуру по полю зображення.

В [29] представлені ознаки, які базуються на вимірі довжин однакових серій елементів контуру. Згідно до того ж джерела, довжина серії – це число елементів рядка растра, що мають постійну яскравість. Нехай $C_p(i,j)$ означає кількість ліній, довжина яких рівна j, та які орієнтовані в напрямку ρ.

Ці лінії складаються з точок зображення, рівні інтенсивності яких лежать в i-му інтервалі. Тоді можна виділити наступні ознаки:

– вага ліній, що мають постійну оптичну щільність, тобто: $T_{29} = \dfrac{\sum_{i,j} j^2 C_\rho(i,j)}{\sum_{i,j} C_\rho(i,j)}$. Ця ознака характеризується тим, що для будь-якого рівня сірого вага кожної лінії збільшується в міру збільшення довжини.

– розподіл рівнів сірого $T_{30} = \dfrac{\sum_i \left(\sum_j C_\rho(i,j) \right)^2}{\sum_{i,j} C_\rho(i,j)}$. Ця ознака має мінімум у тих випадках, коли число ліній постійної оптичної щільності рівномірно розподілене по рівнях сірого;

– розподіл довжини ліній постійної оптичної щільності $T_{31} = \dfrac{\sum_j \left(\sum_i C_\rho(i,j) \right)^2}{\sum_{i,j} C_\rho(i,j)}$ – має мінімум при рівномірному розподілі.

– відносне число ліній постійної оптичної щільності $T_{32} = \dfrac{\sum_{i,j} C_\rho(i,j)}{N_x N_y}$. Значення цієї ознаки максимально, коли всі лінії мають малі довжини.

Розв’язок проблеми вибору інформативних ознак для систем біометричної ідентифікації

Слід зазначити, що не всі розглянуті характеристики однаково інформативні при класифікації тих або інших утворень на зображеннях, які можуть бути використані в системах біометричної ідентифікації. Пояснюється це їх складною програмною реалізацією. У зв’язку з цим, для збільшення обчислювальної ефективності алгоритмів необхідно вирішити завдання аналізу інформативності та оптимізації розширеної системи ознак.

Основне питання при побудові системи ознак полягає в тому, щоб визначити, які та скільки ознак необхідно виділити для надійної класифікації об’єктів на зображенні. При цьому слід керуватися принципом обліку властивостей регулярності об’єкта: якщо об’єкт, який класифікується, має деяку регулярність, то цю регулярність необхідно покласти в основу формування системи ознак. Більш того, необхідно передбачити, щоб ця регулярність була властива всім об’єктам, які належать даному класу [33].

В [38] говориться, що формальної процедури завдання вихідної системи ознак поки не існує. Ознаки, використовувані при розв’язку тих або інших завдань, задаються лише на підставі досвіду та інтуїції фахівця. З обраної таким способом вихідної системи, тим або іншим формальним шляхом вибирається більш економічна та найбільш інформативна підсистема опису образів. Сам же процес завдання вихідної системи ніяк не формалізований. Існує думка, що потрібно задавати все, що тільки можна використати в якості інформативності. Але це вірно тільки в принципі. На практиці ж надмірне роздування вихідної системи ознак не є надто шкідливим через те, що ступінь показності вибірки одного й того ж самого обсягу обернено пропорційна розмірності простору ознак. У випадку використання жорстко встановлених вирішальних функцій, додавання ознак при малій навчальній вибірці може не тільки не поліпшити, але навіть погіршити якість навчання пристрою розпізнавання. Зрозуміло, при необмеженій вибірці, додавання ознаки, що навіть не несе ніякої інформації, ніколи не може погіршити якість розпізнавання.

У проблемі вибору інформативних ознак слід виділити два основні моменти, а саме [38]:

1) необхідно визначити функціонал інформативності підсистеми ознак;

2) необхідно визначити технологію формування послідовностей досліджуваних на інформативність підпросторів ознак.

Насамперед відмітимо, що адекватним завданню оцінювання якості (інформативності) комплексів ознак є лише середній ризик або емпірична оцінка останнього по навчальній вибірці, тобто той же критерій, мінімізацією

якого отримано оптимальне правило розпізнавання образів: у нашому випадку – контурів.

Що стосується способів вибору підпросторів ознак, то різноманітність застосовуваних на практиці способів є невеликою. Зазначимо, що розв'язок поставленого завдання є відомим та тривіальним: для одержання оптимальної підсистеми з k ознак, обраних серед n вихідних компонентів вектора спостереження, потрібно лише зробити порівняння обчислених на різних k-мірних підпросторах значень критерію інформативності та зафіксувати той набір k ознак, на якому обраний критерій досягає оптимуму. Кількість таких підрахунків критерію оптимальності дорівнює числу $\binom{n}{k}$ – комбінацій з n ознак по k. Але навіть для порівняно невеликих k та n, кількість підрахунків становить астрономічні цифри щодо витрат машинного часу.

Зважаючи на сказане, на практиці широко застосовуються способи усічених переборів підпросторів ознак. Так, в алгоритмі, який умовно назвемо «А», може виконуватися усічений перебір. При такому переборі система ознак скорочується шляхом послідовного виключення малоінформативних ознак.

У варіанті «Б» система інформативних ознак може набиратися послідовно шляхом послідовного включення високоінформативних ознак.

В [39] показана практична реалізація комбінованого алгоритму вибору інформативних підпросторів k ознак. Він являє собою модифікований варіант усіченого перебору. Процес розширення системи ознак блоками триває доти, поки інформативна сукупність $i + j + ...l$ k ознак не досягне шуканої величини k. В окремому випадку, зважаючи на $i = j = ... = l = 1$, можна отримати алгоритм «Б».

Аналогічне узагальнення допускає алгоритм усіченого перебору підпросторів «А», у якому скорочення вихідної розмірності n також здійснюється блоками в режимі умовно повного перебору. Тим самим пропонований алгоритм дозволяє розглядати додаткові варіанти просторів ознак та досліджувати їх на інформативність.

На закінчення підрозділу відзначимо тенденції в розвитку методів опису контурів, як одного з різновидів опису загальних текстур зображень.

Як випливає з [29], останнім часом з’являється усе більше робіт з аналізу кольорових зображень та динамічних текстур. При аналізі кольорових зображень для опису контурів уводяться додаткові ознаки, засновані на вимірі рівнів інтенсивності кожного кольору та їх розподілу по полю зображення. При аналізі динамічних текстур, які змінюються в часі, уводиться фактор часу, що представляє собою третій вимір. Він додається до двох просторових координат. У цьому випадку всі зміни контурних ліній моделюються переміщенням окремих незмінних частин (зрушенням, обертанням і т.д.).

Сучасний стан проблеми аналізу та виділення контурних ліній на зображеннях характеризується різноманіттям пропонованих методів, що пояснюється як широким діапазоном розглянутих об’єктів розпізнавання, так і різним характером розв’язуваних завдань. Далі в роботі показано, що найбільш доцільними та наочними ознаками для розв’язку завдання біометричної ідентифікації, виявилися ознаки, які базуються на побудові одномірних гістограм. При цьому показана необхідність попередньої обробки зображень з метою поліпшення якості розпізнавання та його ймовірності.

Висновки до розділу 1

Розглядаючи особливості інформаційної функції системи управління економічною безпекою підприємства, слід зазначити, що тільки системний підхід до управління підприємництвом і безпекою в ньому, коли всі працівники зобов'язані, особливо в кризових, конфліктних і нестабільних ситуаціях, серйозно ставитися до проблеми забезпечення інформаційної, особистої безпеки та економічної безпеки організації в цілому, спричинить позитивні результати діяльності. Для цього менеджеру і фахівцям служби безпеки організації необхідно ретельно освоїти й ефективно застосовувати основні способи управління організацією, персоналом і системою безпеки підприємств та організацій сфери економіки, бізнесу та фінансів. Отже, для нормального розвитку необхідно не тільки створити систему безпеки підприємства, а й уміло і професійно управляти нею.

Інформаційна безпека підприємств та організацій сфери економіки, бізнесу та фінансів забезпечується шляхом проведення цілісної державної програми відповідно до Конституції та чинного законодавства України і норм міжнародного права шляхом реалізації відповідних доктрин, стратегій, концепцій і програм, що стосуються національної інформаційної політики України. Поняття інформаційної безпеки підприємства слід також розглядати в контексті забезпечення безпечних умов існування інформаційних технологій, що включають питання захисту інформації, побудови ефективної інформаційної інфраструктури, інформаційного ринку та створення безпечних умов існування і розвитку інформаційних процесів.

Встановлено, що централізоване управління ідентифікаційною інформацією, корпоративною політикою безпеки та захистом корпоративних мереж і міжмережевих взаємодій для підприємств та організацій сфери економіки, бізнесу та фінансів, а також для інших зацікавлених фізичних та юри-

дичних осіб – це ті три основних компоненти на які спирається безпека будь-якого бізнесу.

Показано, що у зв'язку з постійно зростаючою кількістю корпоративних додатків, що вимагають розмежування прав доступу, розгортання централізованого управління ідентифікаційною інформацією забезпечує відчутне зростання продуктивності підприємств, зменшуючи при цьому витрати, пов'язані з управлінням так званим «ідентифікаційним хаосом» різнорідних додатків. Відповідно, для вирішення окремих завдань стосовно зазначеного, отримані рішення, призначені для інтеграції розрізнених систем ідентифікації користувачів в складі гетерогенних систем на базі єдиного корпоративного каталогу та побудови централізованої системи управління правами доступу користувачів на основі принципів рольового доступу.

Отримані рішення дозволяють в майбутньому здійснювати такі функції:

– проводити аутентифікацію та авторизацію користувачів гетерогенних систем на основі біометричних пристроїв;

– виконувати централізоване адміністрування процесу реєстрації облікових записів користувачів, у тому числі – самообслуговування користувачем його персональної інформації;

– централізоване управління правами доступу користувачів на основі їх бізнес- ролей;

– централізований аудит привілеїв користувачів, включаючи привілеї груп, в які він входить, ролей, які йому призначені, і переліку доступних йому ресурсів;

– делегування повноважень адміністраторам окремих додатків, груп, територіальних об'єднань і т. д.

Науковою новизною отриманих результатів у сенсі управління ідентифікаційною інформацією і доступом є упорядкування і централізація процедури доступу до додатків і мережевих сервісів на основі актуальних ідентифікаційних даних користувачів.

Практичне значення результатів полягає у зниженні адміністративних витрат на розгортання, інтеграцію і підтримку механізмів управління доступом користувачів до різних корпоративних додатків і платформ, а також істотне зростання рівня захищеності інформаційних ресурсів підприємств та організацій сфери економіки, бізнесу та фінансів за рахунок усунення «ідентифікаційного хаосу» використовуваних різнорідних додатків і платформ.

Отримані результати, у відповідності до вище зазначених наукової новизни та практичного значення, відповідають рівню аналогічних розробок, отриманих науковими приацівниками та вченими світового рівня. Їх достовірність, точність та коректність підтверджені достатньою кількість наукових публікацій у виданнях за переліками ВАК України та у виданнях, що входять до міжнародних науковометричних баз даних.

РОЗДІЛ 2

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА ФІНАНСОВО-ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВ

2.1. Загальні принципи побудови системи безпеки підприємства

Створенню служби безпеки підприємства, як правило, передують дві події:

1) гостре бажання керівників підприємства відреагувати на раптово виниклі реальні загрози майну, фізичної розправи з персоналом і т.д.;

2) заснований на результатах дослідження висновок про незадовільний стан безпеки підприємства.

У першому випадку створена поспішно служба безпеки здатна в деякій мірі дати відсіч загрозі та надалі реагувати на їх появу за принципом «загроза-відсіч».

Справа істотно змінюється при реалізації другого варіанту. Після детального вивчення стану безпеки підприємства (із залученням фахівців, якщо їх немає на підприємстві) у його керівників з’явиться реальне уявлення про систему безпеки підприємства.

Таке системне уявлення (зафіксоване в письмовій формі) дозволяє усвідомлено і цілеспрямовано проводити роботу щодо забезпечення безпеки діяльності підприємства всіма його підрозділами й співробітниками. При цьому провідна роль служби безпеки не зникає, навпаки, розуміння своєї ролі і місця в системі безпеки підприємства призведе тільки до позитивних результатів.

Слід, однак, підкреслити, що до теперішнього часу немає єдиного підходу до визначення поняття «система безпеки підприємства». Щоб дати таке визначення, необхідно попередньо виявити елементи цієї системи. Вивчення спеціалізованої літератури і практики дозволили прийти до висновку, що структурними елементами системи безпеки підприємства є:

– наукова теорія безпеки підприємства;

– політика і стратегія безпеки;

– засоби та методи забезпечення безпеки;

– концепція безпеки підприємства.

Сукупність перерахованих вище елементів складає *систему безпеки підприємства*.

Наукова теорія безпеки підприємства, строго кажучи, знаходиться в стадії формування. Відноситься це, насамперед, до понятійного апарату. Дамо аналіз деяких принципових понять.

У російському законодавстві (українське в цьому плані, на жаль, значно відстає) поняття безпеки наведено у ст. 1 Закону Російської Федерації від 5 березня 1992 року «Про безпеку»: «стан захищеності життєво важливих інтересів особистості, суспільства і держави від внутрішніх і зовнішніх загроз». Розкриття цього поняття терміном «захищеність» значно звужує її зміст, підкреслює пасивність при реагуванні на загрози. Сутність безпеки, як виявляється, пов'язана з поняттями «розвиток» і «стійкість». У зв'язку з цим під безпекою далі будемо розуміти стан об'єкта (у нашому випадку – підприємства або організації профілем діяльності якого є економіка, бізнес та фінанси) у системі його зв'язків з точки зору здатності до стійкості (самовиживання) і розвитку в умовах внутрішніх і зовнішніх загроз, дій непередбачуваних і важко прогнозованих факторів. Відштовхуючись від цього поняття, визначимо такі функції безпеки: *виявлення, попередження, зниження, ослаблення, нейтралізація, припинення, локалізація, відображення* та *усунення загроз*.

Під *загрозою безпеки підприємства* будемо розуміти потенційно або реально можлива подія, дія, процес або явище, яке здатне порушити його стійкість і розвиток або призвести до зупинки його діяльності.

Загрози можна класифікувати по різних підставах і вимірювати їх у кількісних параметрах. Наприклад, можливий збиток оцінюється числом загиблих людей, що втратили здоров'я, грошовій сумі економічних втрат і т.д.

За ступенем ймовірності загроза може оцінюватися як неймовірна, малоймовірна, ймовірна, вельми ймовірна і цілком ймовірна. За ступенем роз-

витку загроза проходить чотири етапи: *виникнення (зародження), експансія, стабілізація* і *ліквідація*.

Віддаленість загрози у часі визначається як *безпосередня, близька (до 1 року)* і *далека (понад 1 року)*, а віддаленість у просторі – *територія підприємства, прилегла до підприємства територія, територія регіону, територія країни, зарубіжна територія*. Темпи наростання загрози вимірюються по *місяцях, кварталах, роках*. Напруженість загрози відбивається у двох вимірах:

а) нормальна, підвищена, близька до межі (поріг), надлишкова;

б) зростання, стабільність або зниження.

Крім цього, загрози діляться за природою їх виникнення на два класи:

1) природні (об'єктивні), тобто викликані стихійними природними явищами, не залежними від людини (повені, землетруси, урагани і т.п.);

2) штучні (суб'єктивні), тобто викликані діяльністю людини, ненавмисні (ненавмисні) і навмисні (умисні) загрози.

Розрізняють також *економічні, соціальні, правові, організаційні, інформаційні, екологічні, технічні* та *кримінальні загрози*.

Під *об'єктом безпеки підприємства* слід розуміти *ступінь стійкості* і *розвитку підприємства, його здатність протистояти загрозам*. В об'єкти безпеки підприємства можна виділити:

– різні структурні підрозділи або групи співробітників, або власники акцій підприємства;

– ресурси підприємства (інформаційні, кадрові, матеріально-технічні, інформаційні, інтелектуальні та фінансові);

– різні види діяльності (управлінська, виробнича, постачальна і т.д.).

Метою забезпечення безпеки підприємства є комплексний вплив на потенційні і реальні загрози, що дозволяє йому успішно функціонувати в нестабільних умовах зовнішнього і внутрішнього середовища.

Досягнення цієї мети вимагає реалізації таких завдань:

– виявлення загроз для стабільності й розвитку підприємства і вироблення заходів щодо їх протидії;

– забезпечення захисту технологічних процесів;

– реалізація заходів протидії всіх видів шпигунства (промислового, науково-технічного, економічного і т.д.);

– своєчасне інформування керівництва підприємства про факти порушення законодавства з боку державних і муніципальних органів, комерційних і некомерційних організацій, які зачіпають інтереси підприємства;

– попередження переманювання співробітників підприємства, що володіють конфіденційною інформацією;

– всебічне вивчення ділових партнерів;

– своєчасне виявлення та адекватне реагування на дезинформаційні заходи;

– розробка і вдосконалення локальних правових актів, спрямованих на забезпечення безпеки підприємства;

– реалізація заходів щодо захисту комерційної та іншої інформації;

– організація заходів з протидії недобросовісній конкуренції;

– забезпечення захисту всіх видів ресурсів підприємства;

– реалізація заходів щодо захисту інтелектуальної власності;

– організація та проведення заходів щодо запобігання надзвичайних ситуацій;

– виявлення негативних тенденцій серед персоналу підприємства, інформування про них керівництва підприємства і розробка відповідних рекомендацій;

– організація взаємодії з правоохоронними і контрольними органами з метою попередження і припинення правопорушень, спрямованих проти інтересів підприємства;

– розробка та реалізація заходів щодо попередження загроз фізичній безпеці майну підприємства і його персоналу;

– відшкодування матеріальної та моральної шкоди, завданої підприємству в результаті неправомірних дій організацій і окремих фізичних осіб.

Система безпеки підприємства може бути побудована на основі наступних принципів:

1) ***Пріоритет заходів попередження.*** Зміст цього принципу передбачає своєчасне виявлення тенденцій і передумов, що сприяють розвитку загроз, на основі аналізу яких виробляються відповідні профілактичні заходи щодо недопущення виникнення реальних загроз.

2) ***Законність.*** Заходи безпеки підприємства розробляються на основі і в рамках чинних правових актів. Локальні правові акти підприємства не повинні суперечити законам і підзаконним актам.

3) ***Комплексне використання сил і засобів.*** Для забезпечення безпеки використовуються всі наявні в розпорядженні підприємства сили та засоби. Кожен співробітник повинен в рамках своєї компетенції брати участь у забезпеченні безпеки підприємства. Організаційною формою комплексного використання сил і засобів є програма забезпечення безпеки підприємства.

4) ***Координація та взаємодія всередині і поза підприємством.*** Заходи протидії загрозам здійснюються на основі взаємодії та скоординованості зусиль всіх підрозділів, служб підприємства, а також встановлення необхідних контактів із зовнішніми організаціями, здатними надати необхідне сприяння в забезпеченні безпеки підприємства.

5) ***Поєднання гласності з конспірацією.*** Доведення до відома персоналу підприємства та громадськості в допустимих межах заходів безпеки виконує найважливішу роль – запобігання потенційних і реальних загроз. Така гласність, однак, повинна неодмінно доповнюватися в виправданих випадках заходами конспіративного характеру.

6) ***Компетентність.*** Співробітники та групи співробітників повинні вирішувати питання забезпечення безпеки на професійному рівні, а в необхідних випадках – спеціалізуватися по основних його напрямках.

7) ***Економічна доцільність.*** Вартість фінансових витрат на забезпечення безпеки не повинна перевищувати той оптимальний рівень, при якому втрачається економічний сенс їх застосування.

8) ***Планова основа діяльності.*** Діяльність по забезпеченню безпеки повинна будуватися на основі комплексної програми забезпечення безпеки під-

приємства, підпрограм забезпечення безпеки по основних його видах (економічна, науково-технічна, екологічна, технологічна і т.д.) і розроблюваних для їх виконання планів роботи підрозділів підприємства та окремих співробітників.

9) ***Системність.*** Цей принцип передбачає врахування всіх факторів, що впливають на безпеку підприємства, включення в діяльність щодо його забезпечення всіх співробітників підрозділів, використання в цій діяльності всіх сил і засобів.

Система безпеки підприємства включає в себе ряд наступних підсистем:

Економічна безпека – стан найбільш ефективного використання всіх видів ресурсів з метою запобігання (нейтралізації, ліквідації) загроз і забезпечення стабільного функціонування підприємства в умовах ринкової економіки.

Техногенна безпека – сукупність дій по забезпеченню проектування, будівництва та експлуатації складних технічних пристроїв з дотриманням необхідних вимог безаварійної їх роботи.

Екологічна безпека – стан захищеності життєво важливих інтересів персоналу підприємства і його майна від потенційних або реальних загроз, що створюються наслідками антропогенного впливу на навколишнє середовище, а також від стихійних лих і катастроф.

Інформаційна безпека – це здатність персоналу підприємства забезпечити захист інформаційних ресурсів і потоків від загроз несанкціонованого доступу до них.

Психологічна безпека – стан захищеності від негативних психологічних впливів персоналу підприємства та інших осіб, залучених до її діяльності.

Фізична безпека – стан захищеності життя і здоров'я окремих осіб (груп, всіх осіб) підприємства від насильницьких злочинів.

Науково-технічна безпека – здатність персоналу підприємства забезпечити захист власної цінної науково-технічної продукції від недобросовісних конкурентів.

Пожежна безпека – стан об'єктів підприємства, при якому заходи попередження пожеж та протипожежного захисту відповідають нормативним вимогам.

Слід зазначити, що вищевказані підсистеми другого рівня можуть включати в себе підсистеми третього рівня. Наприклад, підсистемами економічної безпеки можуть бути – фінансова, комерційна, майнова, а також інші підсистеми безпеки.

Крім цього, самі підсистеми не розділені між собою непрохідною кордоном, оскільки вони настільки взаємопов'язані один з одним, що в органічній єдності утворюють єдину систему безпеки підприємства. Поділ же єдиної системи безпеки підприємства на підсистеми другого і третього рівня проводиться з методичних міркувань, оскільки це дозволяє більш детально вивчити всі його елементи.

Надійність і ефективність системи безпеки підприємства оцінюється на основі одного критерію – ступеня відсутності або наявності завданої йому матеріальної шкоди та моральної шкоди. Зміст цього критерію розкривається через ряд показників:

1) недопущення фактів витоку конфіденційних відомостей;

2) попередження або припинення протиправних дій з боку персоналу підприємства, його відвідувачів, клієнтів;

3) збереження майна та інтелектуальної власності підприємства;

4) попередження надзвичайних ситуацій;

5) припинення насильницьких злочинів відносно окремих (спеціально виділених) співробітників і груп співробітників підприємства;

6) своєчасне виявлення і припинення спроб несанкціонованого проникнення на охоронювані об'єкти підприємства.

2.2. Політика та стратегія безпеки

2.2.1. Основи політики безпеки підприємства

Політика безпеки підприємства – це загальні орієнтири для дій і прийняття рішень, які полегшують досягнення цілей. Т.ч., для встановлення цих загальних орієнтирів необхідно спочатку сформулювати цілі забезпечення безпеки підприємства (загальна мета нами вже визначена раніше). Такими цілями можуть бути:

– зміцнення дисципліни праці і підвищення його продуктивності;

– захист законних прав та інтересів підприємства;

– зміцнення інтелектуального потенціалу підприємства;

– збереження та примноження власності;

– підвищення конкурентоспроможності виробленої продукції;

– максимально повне інформаційне забезпечення діяльності підприємства і підвищення його ефективності;

– орієнтація на світові стандарти і лідерство в розробці та освоєнні нових технологій;

– виконання виробничих програм;

– надання сприяння управлінським структурам у досягненні цілей підприємства;

– недопущення залежності від випадкових і несумлінних ділових партнерів.

З урахуванням вищевикладеного можна визначити наступні загальні орієнтири для дій і прийняття рішень, які полегшують досягнення цих цілей:

– збереження і нарощування ресурсного потенціалу;

– проведення комплексу превентивних заходів щодо підвищення рівня захищеності власності і персоналу підприємства;

– включення в діяльність по забезпеченню безпеки підприємства всіх його співробітників;

– професіоналізм і спеціалізація персоналу підприємства;

– пріоритетність несилових методів запобігання і нейтралізації загроз.

Для успішного виконання цієї політики необхідно реалізувати стратегію безпеки підприємства, під якою розуміється сукупність найбільш значущих рішень, спрямованих на забезпечення прийнятного рівня безпеки функціонування підприємства.

Виділяються такі ***типи стратегій безпеки***:

1) орієнтовані на усунення існуючих або запобігання виникнення можливих загроз;

2) націлені на запобігання впливу існуючих або можливих загроз на предмет безпеки;

3) спрямовані на відновлення (компенсацію) завданої шкоди.

Перші два типи стратегій передбачають таку діяльність із забезпечення безпеки, в результаті якої не виникає загрози або створюється заслін її впливу. У третьому випадку збиток допускається (виникає), проте він компенсується діями, які передбачає відповідна стратегія. Цілком очевидно, що стратегії третього типу можуть розроблятися і реалізовуватися стосовно ситуацій, де збитки можуть бути компенсовані, або тоді, коли немає можливості здійснити будь-яку програму реалізації стратегій першого або другого типу.

2.2.2. Суб'єкти безпеки підприємства

Забезпеченням безпеки підприємства займаються дві групи суб'єктів.

Перша група займається цією діяльністю безпосередньо на підприємстві і підпорядкована його керівництву. Серед цієї групи виділяють спеціалізовані суб'єкти (рада або комітет безпеки підприємства, служба безпеки, пожежна частина, рятувальна служба і т.д.), основним призначенням яких є постійна професійна діяльність щодо забезпечення безпеки підприємства (у рамках своєї компетенції). Іншу частину суб'єктів цієї групи умовно можна назвати напівспеціалізованою, так як частина функцій цих суб'єктів призначена для

забезпечення безпеки підприємства (медична частина, юридичний відділ і т.д.). До третьої частини цієї групи суб'єктів належить увесь інший персонал і підрозділи підприємства, які в рамках своїх посадових інструкцій і положень про підрозділи зобов'язані вживати заходів до забезпечення безпеки. Слід мати на увазі, що ефективно забезпечувати безпеку підприємства ці суб'єкти можуть тільки в тому випадку, якщо цілі, завдання, функції, права і обов'язки будуть розподілені між ними Т.ч., щоб вони не перетиналися один з одним.

До другої групи суб'єктів відносяться зовнішні органи та організації, які функціонують самостійно і не підкоряються керівництву підприємства, але при цьому їх діяльність має суттєвий (позитивний чи негативний) вплив на безпеку підприємства. Суб'єктами цієї групи є:

– законодавчі органи;

– органи виконавчої влади;

– суди;

– правоохоронні органи;

– науково-освітні установи.

Останні (особливо недержавні установи з підготовки приватних охоронців) покликані забезпечити науково-методичне опрацювання проблем безпеки підприємства та підготовку відповідних фахівців у сфері безпеки підприємств.

Очевидно, що суб'єкти другої групи за своєю ініціативою підключаються епізодично (або ніколи) до діяльності підприємства із забезпечення своєї безпеки. Організаційною формою такого підключення може стати *комплексна програма безпеки підприємства*, в якій необхідно передбачити форми і методи цієї роботи. Крім того, можна рекомендувати розробку планів структурних підрозділів і всього підприємства в цілому по організації взаємодії з вищевказаними органами та організаціями.

2.2.3. Засоби та методи забезпечення безпеки

Серед існуючих засобів забезпечення безпеки виділимо наступні:

1) ***Технічні засоби.*** До них відносяться охоронно-пожежні системи, відео-радіоапаратура, засоби виявлення вибухових пристроїв, бронежилети, загородження і т.д.

2) ***Організаційні засоби.*** Створення спеціалізованих оргструктурних формувань, що забезпечують безпеку підприємства.

3) ***Інформаційні засоби.*** Насамперед, це друкована та відеопродукція з питань збереження конфіденційної інформації. Крім цього, найважливіша інформація для прийняття рішень з питань безпеки зберігається в комп'ютерах.

4) ***Фінансові кошти.*** Цілком очевидно, що без достатніх фінансових коштів неможливе функціонування системи безпеки: питання лише в тому, щоб використовувати їх цілеспрямовано і з високою віддачею.

5) ***Правові засоби.*** Тут мається на увазі використання не тільки виданих вищими органами влади законів і підзаконних актів, але й розробка власних, так званих локальних правових актів з питань забезпечення безпеки.

6) ***Кадрові кошти.*** Мається на увазі насамперед достатність кадрів, що займаються питаннями забезпечення безпеки. Одночасно з цим вирішують завдання підвищення їх професійної майстерності в цій сфері діяльності.

7) ***Інтелектуальні засоби.*** Залучення до роботи висококласних фахівців, науковців (іноді доцільно залучати їх з боку) дозволяє впроваджувати нові системи безпеки.

Зауважимо, що застосування кожного з вищевказаних засобів окремо не дає необхідного ефекту: він можливий тільки на комплексній основі. У той же час необхідно відзначити, що одночасне використання всіх вищевказаних коштів в принципі неможливо. Воно проходить зазвичай ряд етапів:

I : виділення фінансових коштів;

II : формування кадрових і організаційних засобів;

III : розробка системи правових засобів.

IV : залучення технічних, інформаційних та інтелектуальних засобів.

Перекладені з статичного в динамічний стан вищевказані кошти стають методами, тобто прийомами, способами дії. Відповідно, можна говорити про технічні, організаційні, інформаційні, фінансові, правові, кадрові та інтелектуальні методи. Наведемо короткий конкретний перелік цих методів:

– ***технічні*** – спостереження, контроль, ідентифікація і т.д.;

– ***організаційні*** – створення зон безпеки, режим, розслідування, пости, патрулі і т.д.;

– ***інформаційні*** – складання характеристик на співробітників, аналітичні матеріали конфіденційного характеру тощо;

– ***фінансові*** – матеріальне стимулювання співробітників, що мають досягнення в забезпеченні безпеки, грошове заохочення інформаторів і т.д.;

– ***правові*** – судовий захист законних прав та інтересів, сприяння правоохоронним органам і т.д.;

– ***кадрові*** – підбір, розстановка і навчання кадрів, які забезпечують безпеку підприємства, їх виховання і т.д.;

– ***інтелектуальні*** – патентування, ноу-хау і т.д.

2.2.4. Концепція безпеки підприємства

Після вивчення всіх вищеописаних елементів системи безпеки підприємства необхідно перейти до складання й концепції.

Концепція визначається як система поглядів, ідей, цільових установок, пронизаних єдиним, визначальним задумом, провідною думкою, що містить постановку і шляхи вирішення виявлених проблем.

В подальшому під поняттям «концепція» розумітимемо концепцію предметної області досліджень, тобто *концепцію безпеки підприємства*.

До будь-якої концепції можна встановити такі вимоги:

1) **Конструктивність.** Така вимога буде визнана реалізованою, якщо в концепції знаходять відображення:

– початковий стан об’єкта, на перетворення якого спрямована концепція;

– стан об’єкта, досягнутий в результаті реалізації концепції;

– заходи, необхідні для досягнення сформульованих у концепції цілей;

– кошти, необхідні і достатні для досягнення поставлених цілей;

– джерела ресурсного забезпечення, що використовуються в ході реалізації концепції;

– механізм реалізації концепції, тобто способи (методи) використання виділених коштів і ресурсів.

2) **Сумісність.** Мається на увазі те, що концепція перетворення якого-небудь об’єкту повинна гармонійно вписуватися в систему перетворень взаємопов’язаних в єдину систему об’єктів, одним з компонентів якої він є.

3) **Відкритість.** Розроблена концепція повинна давати можливість в її рамках реагувати на зміну умов реалізації концепції і вносити корективи в реалізацію в разі їх необхідності.

Вищевказані вимоги диктують в якості ***обов’язкової умови*** включення в логічну структуру концепції наступних позицій:

– виявлення об’єкта і предмета, визначення їх сутності, місця серед множини інших;

– чітке формулювання ролі реалізації концепції і завдань, що стоять при її реалізації;

– виділення умов, необхідних і достатніх для реалізації концепції, і зіставлення їх з реально існуючими;

– визначення кола заходів, що забезпечують перетворення об’єкта реалізації концепції, а також шляхів її реалізації;

– формулювання критеріїв успішності заходів щодо розробки концепції, а також з оцінки результатів її реалізації.

Концепція безпеки підприємства являє собою офіційно затверджений документ, в якому відображена система поглядів, вимог і умов організації заходів безпеки персоналу і власності підприємства. Орієнтовна структура концепції може виглядати наступним чином:

Опис проблемної ситуації у сфері безпеки підприємства

– перелік потенційних і реальних загроз безпеці, їх класифікація і ранжування;

– причини та фактори зародження загроз;

– негативні наслідки загроз для підприємства.

Механізм забезпечення безпеки

– визначення об'єкта і предмета безпеки підприємства;

– формулювання політики і стратегії безпеки;

– принципи забезпечення безпеки;

– мета забезпечення безпеки;

– завдання забезпечення безпеки;

– критерії та показники безпеки підприємства;

– створення організаційної структури з управління системою безпеки підприємства.

Заходи з реалізації заходів безпеки

– формування підсистем загальної системи безпеки підприємства;

– визначення суб'єктів безпеки підприємства та їх ролі;

– розрахунок коштів та визначення методів забезпечення безпеки;

– контроль і оцінка процесу реалізації концепції.

Необхідно мати на увазі, що найбільш повне уявлення про систему безпеки підприємства можна отримати після вивчення офіційно прийнятих документів по концепції безпеки підприємства, комплексної програми забезпечення безпеки підприємства та планів підрозділів підприємства з реалізації цієї програми. Сформована на науковій основі система безпеки підприємства є організаційною основою створення її структурного підрозділу – служби безпеки.

2.3. Економічна безпека господарюючих суб‘єктів муніципального утворення

Розвиток економіки під впливом ринкових механізмів виділило в якості самостійної функцію держави щодо захисту економічної безпеки. Ринкові механізми не в змозі виконувати дану функцію. Як правило, економічні інтереси господарюючих суб’єктів не суперечать національним інтересам. Однак такі суперечності можуть часто виникають у результаті господарської діяльності. Наприклад, ринкові механізми роблять вигідним розвиток екологічно шкідливих виробництв, а держава зацікавлена стримувати їх розвиток і імпортувати відповідну про продукцію. Для вирішення подібних протиріч держава повинна здійснювати свою функцію забезпечення економічної безпеки.

Держава може забезпечити лише захист від найбільш важливих і великих загроз. Населення ж у своєму повсякденному житті стикається зі значно більшим спектром загроз, багато з яких носять місцевий характер. Захистити населення від багатьох подібних місцевих загроз економічній безпеці найбільш ефективним чином можуть органи місцевого самоврядування, як органи найбільш наближені до населення.

Об’єктами економічної безпеки муніципального утворення є його територія, населення і все, що відноситься до економіки, яке розташоване на даній території: ділянці земної поверхні, що має окремі межі і просторовий базис діяльності, який включає виробничі фонди, інфраструктуру, та розглядається як середовище життєдіяльності населення і сукупність ресурсів розвитку.

Об’єктом дослідження економічної безпеки на муніципальному рівні є кругообіг витрат і доходів, товарів, послуг і ресурсів на основі різних форм власності. Підставою для оцінки загроз та збитків від впливу загроз як прийнятних, так і неприйнятних, є критерії економічної безпеки, які можуть бути якісними або кількісними.

Критерії, в свою чергу, виражаються показниками економічної безпеки. Т.ч., ***сутність економічної безпеки*** реалізується в системі її критеріїв і показників.

Враховуючи особливості проблем забезпечення муніципальної економічної безпеки, необхідно виробити особливу систему параметрів, орієнтовану на невелику територію. Існуючі системи показників оцінки економічної безпеки орієнтовані, в основному, на державний (в Російській Федерації та країнах з федеративною побудовою – на федеральний) та регіональний рівні. Проте враховуючи важливість і специфічні особливості муніципальних проблем, представляється необхідним спеціальне опрацювання проблем показників безпеки для муніципальних утворень. Цілями застосування подібної методики є:

– оцінка кризових ситуацій та загрози їх виникнення в соціально-економічній сфері муніципального утворення;

– оцінка впливу місцевих кризових ситуацій на національну безпеку суб'єкта господарювання і країни в цілому;

– розробка та обґрунтування програмно-цільових заходів щодо забезпечення економічної безпеки.

Основні вимоги до системи соціально-економічних показників аналізу муніципального утворення:

– система соціально-економічних показників муніципального утворення повинна бути взаємопов'язана із загальною схемою аналізу та показників, які використовуються на державному, регіональному та галузевому рівнях;

– показники муніципальної безпеки повинні бути сумісні з діючою в країні системою обліку, статистики та прогнозування;

– система соціально-економічних показників повинна відповідати переліку основних загроз економічній безпеці муніципального утворення;

– перелік соціально-економічних показників, які використовуються для аналізу, повинен бути мінімальним, легко доступним та допускати просту інтерпретацію;

– результати аналізу повинні допускати просту і наочну перевірку на несуперечність існуючим положенням;

– соціально-економічні показники повинні ставитися до одного часового періоду, описуючи свого роду зрізи соціально-економічної ситуації;

– показники повинні допускати можливість здійснювати регулярний моніторинг і прогнозування факторів, що впливають на рівень загроз безпеки муніципального утворення.

Аналіз становища в муніципальному утворенні повинен спиратися на набір індикаторів економічної безпеки, який дозволить виявити і оцінити прийдешні загрози, а також формалізувати необхідний комплекс програмно-цільових заходів щодо зниження рівня загроз.

Критерій економічної безпеки – оцінка стану економіки з точки зору найважливіших процесів, що відображають сутність економічної безпеки. Критерій не може прийматися як пряме керівництво до дії. Необхідно застосовувати гнучкий підхід до його коригування та реалізації відповідно до періодичної перебудови ресурсно-виробничого потенціалу, створенням нових господарських важелів, структур управління.

На думку більшості дослідників, основою формування цих показників є тісний взаємозв’язок поняття безпеки з категорією ризику.

Концепція ризику в стратегії економічної безпеки включає в себе два найважливіших елементи:

1) оцінку ризику;

2) керування ризиком.

Оцінка ризику носить, як правило, експертний, імовірнісний характер.

Управління ризиком припускає передбачення можливих критичних соціально-економічних ситуацій з тим, щоб запобігти, послабити і пом’якшити їх наслідки.

Виходячи зі сказаного, *оцінка рівня економічної безпеки* припускає поряд з аналізом факторів ризику використання категорій втрат (шкоди) фактичних, очікуваних, потенційних, таких, що компенсуються, і таких, які не компенсуються.

Критерії економічної безпеки диктують вибір встановлених показників економічної безпеки об'єкта дослідження, які будуть описувати і характеризувати його еволюцію, рівень його кількісних і якісних параметрів у системі світової статистики. Для економічної безпеки важливе значення мають не самі показники, а їх порогові значення, тобто граничні величини, недотримання значень яких заважає нормальному ходу розвитку різних елементів виробництва, призводить до формування негативних, руйнівних тенденцій для муніципального утворення. Т.ч., показники, за якими визначено порогові значення, виступають у якості ***системи показників економічної безпеки***.

До основних критеріїв, що характеризують інтереси муніципального утворення в галузі безпеки і забезпечують прийнятні для більшості населення умови життя і розвитку особистості, стійкість соціально-економічної ситуації, належать:

– розширене відтворення економічної та соціальної інфраструктури, муніципальної економіки;

– межі критичної залежності муніципального утворення від ввезення найважливіших видів продукції першої необхідності;

– забезпечення необхідного рівня обслуговування потреб населення з метою формування умов для нормального життєзабезпечення населення муніципального утворення.

Виявлення загроз економічній безпеці муніципального утворення і прогнозування їх наслідків здійснюється за допомогою *моніторингу*.

У розпорядженні місцевої влади постійно повинен бути інструментарій аналізу потенційних і реальних загроз економічній безпеці, альтернативний набір вирішення даних проблем.

Найважливішою проблемою, від вирішення якої залежить розробка ефективних заходів політики місцевих органів влади з попередження збитків, є визначення системи порогових рівнів зниження економічної безпеки у відповідь на дію тих чи інших факторів ризику. Наприклад, рівень і якість життя основної маси населення, за межами яких виникає небезпека неконтрольованих соціальних, трудових, міжнаціональних та інших конфліктів, створює загрозу виживанню.

Кожен з основних індикаторів загроз економічній безпеці пов'язаний з оцінкою ситуації в певній сфері. Розрахунок показників, що розглядаються ізольовано один від одного, не дозволяє отримати об'єктивну оцінку. Тільки система показників дозволяє зробити висновки про реальний ступінь загрози економічній безпеці.

Загальноприйнятим вважається, що показовим є зіставлення показників безпеки сусідніх муніципальних утворень. Практика показує, що потрібно не просто визначити чисто макроекономічні індикатори на які важко вплинути в оперативному порядку – їх динаміка складається досить інерційно і під впливом багатьох факторів, які часто не піддаються впливу, – а доцільно використовувати індикатори, які піддаються впливу з боку органів влади як у стратегічному, так і в тактичному плані. Виявляються критичні точки і способи впливу на них.

Критична величина економічних показників безпеки на певній території не завжди означає ситуацію повного краху соціально-економічної сфери або окремих її галузей. Вона, насамперед, свідчить про необхідність оперативного втручання органів управління з метою зміни небезпечних тенденцій.

Можна виділити наступні групи об'єктів для індикативного аналізу економічної безпеки муніципального утворення:

– показники стану інфраструктури (динаміка виробництва, працездатність і ступінь зношеності техніки, технічна аварійність, число об'єктів інфраструктури на 10 000 чоловік та ін.);

– демографія, рівень і якість життя (народжуваність і смертність, тривалість життя, захворюваність; середня та мінімальна заробітна плата і пенсії в порівнянні з прожитковим мінімумом; різниця у рівні доходів між окремими верствами населення; споживання найважливіших видів продовольства і забезпеченість товарами тривалого користування, злочинність та ін.);

– динаміка зайнятості населення, в тому числі по статево-вікових і соціальних групах населення;

– стан фінансово-бюджетної та кредитної системи, забезпеченість фінансовими і матеріальними ресурсами найважливіших муніципальних потреб, забезпеченість ресурсами виконання окремих делегованих державних повноважень;

– дієвість системи державної влади, механізмів правового та адміністративного регулювання;

– стан навколишнього середовища, екологія.

Покажемо більш детально порогові значення індикаторів рівня життя населення, як найбільш важливі для муніципального рівня управління. У цій області часто використовуються наступні показники:

– частка в населенні громадян, що мають доходи нижче прожиткового мінімуму;

– середня тривалість життя;

– розрив між доходами 10% найбільш високодохідних і 10% самих незахищених груп населення;

– рівень народжуваності;

– рівень смертності та захворюваності від різних причин;

– зіставлення середньої заробітна плати і пенсії в даному муніципальному утворенні з прожитковим мінімумом і виплати в сусідніх муніципальних утвореннях;

– рівень безробіття;

– рівень забезпеченості різними товарами тривалого користування;

– рівень злочинності.

При розрахунку показників доходу слід враховувати, що ці дані часто дещо занижені, так як розраховуються тільки на основі грошових доходів населення без врахування натуральних доходів від власних підсобних господарств та без урахування безкоштовних благ і послуг, одержуваних населенням. Крім того, не враховуються багато потоків, які часто перерозподіляються. Зокрема, доходи від неформальної та незареєстрованої зайнятості, від безвідплатної допомоги родичів одне одному. В результаті цієї діяльності населення відбувається перелив доходів від однієї групи населення до іншої.

Проте це не знімає гостроти проблеми з позиції загрози безпеці. Справа в тому, що величина прожиткового мінімуму встановлена на такому низькому рівні, що граничним значенням за цим індикатором мало б бути відсутність громадян, що мають доходи нижче даного рівня. Що стосується розриву в доходах між високо- і малоприбутковими верствами населення, то порогове значення по цьому індикатору попередньо визначається на рівні, який зазвичай приймається в розвинених зарубіжних країнах, де розрив у 8 разів не викликає соціальних конфліктів. Однак населення України звикло до розриву в доходах максимум в 4-5 разів. Тому, по можливості, слід вживати більш жорсткі параметри порогових значень по даному індикатору.

Важливо підкреслити, що найвища ступінь безпеки досягається за умови, що весь комплекс показників перебуває в границях допустимих меж своїх порогових значень, а порогові значення одних показників досягаються не за рахунок інших.

Оцінка інтегрального показника рівня економічної безпеки здійснюється переважно у вигляді табличного представлення де приводяться порівняння основних економічних показників муніципального утворення з їх пороговими значеннями (див. приклад у табл. 2.1):

Таблиця 2.1. Порівняння основних економічних показників муніципального утворення з їх пороговими значеннями

Показник безпеки	**Критичний показник**	**Фактичний показник** (за певний рік)	**Прогнозний показник** (на рік прогнозування)
Рівень безробіття	15%	14%	12%
Знос системи водопостачання та ін.	70%	85%	90%

Порядок використання порогових значень в муніципальному утворенні в узагальненому вигляді представляється наступним. Органи виконавчої влади муніципального утворення розробляють прогнози соціально-економічного розвитку на визначений період, складають проекти бюджету. Перш за все слід встановити, що в цих документах обов'язково повинні міститися показники, які характеризують ступінь економічної безпеки муніципального утворення. У документах має наводитися зіставлення прогнозованих показників соціально-економічного розвитку та бюджету з їх пороговими значеннями. Проекти всіх найбільш важливих рішень з економічних питань також повинні проходити перевірку на предмет відповідності пороговим значенням.

Слід зазначити, що для місцевих органів влади більш показовим і зручним у використанні є функціональний аналіз рівня економічної безпеки. Такий аналіз дозволяє виявити недоліки і резерви реалізованого комплексу заходів щодо забезпечення кожної з функціональних складових економічної безпеки та безпеки території в цілому, а також дати можливість скорегувати функціональну систему забезпечення його економічної безпеки.

Можливий алгоритм аналізу:

1. Визначення структури негативних впливів за кожною функціональною складовою економічної безпеки території. Поділ об'єктивних і суб'єктивних негативних впливів.

2. Оцінка ймовірності настання окремих негативних впливів, а також збитків в разі їх настання з тим, щоб оцінити ймовірний розмір збитку.

3. Формування списку заходів, які було вжито до моменту проведення оцінки рівня економічної безпеки для усунення впливу негативних впливів. Такі списки заходів формуються по кожній з функціональних складових і по кожному негативному впливу всередині кожної складової. Якщо в минулому були прийняті будь превентивні заходи з попередження певних негативних впливів, їх також необхідно включити в список заходів, навіть якщо очікувані негативні впливи так і не мали місця.

4. Оцінка ефективності вжитих заходів з погляду централізації конкретних негативних впливів за кожною з функціональних складових економічної безпеки. Оцінка ефективності прийнятих заходів може проводитися експертами, які проводять загальну оцінку економічної безпеки на даній території або спеціально запрошеними лише для цієї мети, на підставі оцінки відношення економічного ефекту, отриманого від реалізації оцінюваних заходів, попереджуючих за допомогою цих заходів можливих збитків до сукупних витрат на реалізацію комплексу заходів та вартості понесених збитків за функціональною складовою.

5. Визначення причин недостатньої ефективності заходів, прийнятих для усунення вже наявних негативних впливів і запобігання можливим, а також визначення відповідальних за низьку ефективність реалізації прийнятих заходів.

6. Вироблення рекомендацій щодо усунення та попередження негативних впливів.

7. Оцінка вартості кожного з пропонованих заходів з усунення негативних впливів і визначення виконавців, відповідальних за реалізацію запропонованих заходів.

Для виділення найбільш важливих напрямків можна прийняти розрахунок питомої ваги окремих функціональних складових безпеки у загальному збитку (див. табл. 2.2).

Таблиця 2.2. Питома вага окремих функціональних складових безпеки у загальному збитку

Функціональна складова безпеки	**Очікуваний збиток**	**Запобігання шкоди**	**Збиток, що реалізувався**	**Питома вага**
Екологічна	800	100	300	15%
Інформаційна	300	100	160	8%
Фінансова	1500	500	400	20%
і т.д.				57%
Загальний збиток				100%

Приклад аналізу економічної безпеки, що подається в представницький орган влади, наведений у табл. 2.3.

Таблиця 2.3. Приклад аналізу економічної безпеки, що подається в представницький орган влади

Назва негативного впливу	**Імовірність**	**Оцінюваний збиток**	**Ймовірний збиток**
Аварія в системі водопостачання	30%	1000 у.о.	300 у.о.
Перебої в постачанні певного життєво важливого товару	50%	700 у.о.	350 у.о.
Розкрадання проводів і т.д.	90%	500 у.о.	450 у.о.

Представницький орган приймає рішення про те, які негативні впливи слід зменшити в першу чергу. У випадку, якщо негативні впливи не можна подолати за допомогою законодавчих заходів, відповідним виконавчим органам влади дається завдання розробити та подати на розгляд дані відповідно до вимог алгоритму аналізу. На основі даних аналізу представницький орган влади може прийняти рішення про фінансування цільових програм з забезпечення економічної безпеки.

Створення карт функціонального аналізу дозволяє вирішувати одночасно цілу сукупність найважливіших проблем забезпечення економічної безпеки муніципального утворення. Оцінюючи значення фінансових параметрів збитків від очікуваних, реалізуючи заходи з запобігання негативних впливів,

можна отримати достовірне уявлення про масштаби потенційного, понесеного та попередженого збитку від сукупності негативних впливів на економічну безпеку. Також через аналіз питомих ваг функціональних збитків в сукупному збитку можна досить точно оцінити значимість функціональних складових економічної безпеки.

Розрахунок питомих ваг функціональних складових економічної безпеки на основі аналізу збитків дозволяє визначити однорідний параметр дослідження, важко вимірюваний іншими способами функціональних складових економічної безпеки, і тому цей метод є досить ефективним при вирішенні проблеми оцінки функціональних складових економічної безпеки.

Пріоритетними завданнями місцевої політики, спрямованої на підвищення економічної безпеки муніципальних утворень в даний час є:

– підтримка життєво важливих для населення району підприємств та об’єктів інфраструктури;

– забезпечення умов для нормальної життєдіяльності населення;

– надання сприяння переважного розвитку підприємствам, які є найбільш прибутковими і перспективними на даний період, а також підприємствам, які мають довгострокові економічні переваги в загальній системі територіального поділу праці;

– розвиток місцевої інфраструктури.

Розгляд економічної безпеки муніципального утворення повинно здійснюватися в рамках економічної безпеки країни та її суб’єктів.

2.4. Безпека фінансового ринку та фінансової стабільності як суспільне благо

Як відомо (наприклад, з [40]), забезпечення безпеки фінансового ринку та фінансової стабільності входить до числа пріоритетних завдань економічної політики багатьох країн. Це пояснюється тим, що їх безпека сприяє ефективному розміщенню економічних ресурсів та розподілу ризиків, а отже,

стимулює економічну активність та підвищує добробут в країні, що розцінюється як соціальне благо населення. Аналіз стану безпеки у сферах фінансового ринку та фінансової стабільності (далі – *у фінансових сферах*) є порівняно молодим напрямом у сучасній науці. У літературі, наприклад, безпека фінансової стабільності розглядається на трьох рівнях: *мікрорівні, національному* та *міжнародному рівнях*, причому між цими рівнями існує тісний взаємозв'язок. Безпека стабільності на мікрорівні, тобто на рівні окремих організацій, сприяє встановленню фінансової стабільності на національному рівні, у свою чергу безпека фінансової стабільності на національному рівні, тобто на рівні окремих країн, сприяє підтримці фінансової стабільності на міжнародному рівні.

Необхідність аналізу безпеки фінансових сферах на національному рівні обумовлена тим, що її стан на мікрорівні вже досить добре вивчений і в сучасній теорії фінансів підприємства склався певний набір показників для її вимірювання. В той же час стан безпеки у фінансових сферах на національному рівні вимагає подальшого дослідження. Безпека фінансових сфер на міжнародному рівні також залишається недостатньо вивченою, проте її аналіз неможливий без чіткого розуміння того, що є, зокрема, станом фінансової стабільності на національному рівні та як така проблема впливає на суспільний благоустрій.

Питання безпеки у фінансовій сфері на різних рівнях, включаючи національний та міжнародний, присвячений ряд публікацій вітчизняних та зарубіжних авторів. Так, в І. Корміліцина (наприклад, в [40]) викладені підходи до аналізу фінансової стабільності на національному рівні через оцінку чинників чинників та індикаторів, включаючи соціальну сферу. Там же уточнене поняття «фінансова стабільність», описані основні елементи та функції фінансової системи держави, виявлені внутрішні та зовнішні чинники фінансової стабільності і розроблено комплекс індикаторів для кількісної оцінки ризиків. У статтях, авторами яких є М. Арсеньєв [41], відзначається прагнення іноземного фінансового капіталу впливати на спрямованість і темпи реаліза-

ції найважливіших державних програм у галузі оборони, науки і техніки, отримати необмежений доступ до стратегічних мінерально-сировинних ресурсів, до сучасних технологій, нав’язати контракти на поставку застарілих та екологічно шкідливих виробництв і технологій, що істотно позначається на добробуті населення. А. Овчинникова в [42] розкриває основні проблеми економічного росту в рамках постіндустріального технологічного укладу та пропонує нову концепцію економічного зростання в рамках сталого розвитку з урахуванням розвитку трьох взаємодіючих систем – соціальної, екологічної та економічної. Вона відзначає, що незбалансованість фінансового та товарного ринків призводить до цілеспрямованого порушення рівноваги інтересів учасників ринку, спровоковане асиметричністю інформації та трансформацією потреб певної групи індивідів. В [43] В. Ткаченко відзначає, що найбільш високий ступінь фінансової безпеки досягається за умови, коли обрана система показників знаходиться в доступних межах граничних значень, а безпечний рівень одного показника досягається не за рахунок нанесення шкоди іншим показникам. У співавторстві з В. Ткаченко в [44] Є. Коваленко проводить аналіз економічної безпеки регіонів України з урахуванням соціально-економічних факторів і показує її вплив на соціальну сферу. Інші теоретичні, методологічні дослідження та аналіз практики господарювання з проблем фінансової безпеки є об’єктом пильної уваги інших українських вчених-економістів до яких можна віднести О. Барановського, М. Єрмошенко, Н. Фокіної, О. Шнипко, В. Богачова та ін.

Виходячи з аналізу літературних джерел, невирішеною раніше частиною загальної проблеми є розвиток теоретичних питань безпеки фінансового ринку та фінансової стабільності з врахуванням їх впливу на благоустрій населення.

Враховуючи сказане, метою підрозділу звіту є показ того факту, що фінансові ринки та фінансова стабільність є суспільним благом, а держава, як правовий чинник, повинна забезпечити його безпеку.

Загально прийнято вважати, що безпека на фінансовому ринку ототожнюється з його стабільністю. Т.ч., основна мета існування фінансової безпеки

– захист фінансової системи від нестабільностей, викликаних особливостями фінансових криз та системних ризиків. Дестабілізація фінансової системи (так звана *фінансова нестабільність*) – засіб для розрушення економіки в цілому, що явно веде до загрози економічній безпеці.

Економічна безпека, як аспект громадської безпеки, в останні роки стала однією з основних цілей внутрішньої та зовнішньої політики будь-якої держави. Це пов'язано зі зростаючою важливістю економічної безпеки в результаті посилення глобалізації та лібералізації фінансових ринків. Суттєве значення для підтримки економічної безпеки має врахування цих процесів на різних етапах економічного планування та вибір засобів нейтралізації їх негативних наслідків.

Концепція економічної безпеки визначається по-різному для різних вище згаданих рівнів і, як правило, з часом та при подальшому детальному уточненні, змінюються. Поняття про економічну безпеку в цілому можна визначити як здатність держави до розвитку системи «беззагрозності» економіки, тобто стабільного економічного розвитку при відсутності (ліквідації) внутрішніх і зовнішніх економічних загроз. Отже, проведення такої політики економічної безпеки, в ідельному випадку, могло б запобігти порушенням (злочинам) в економічній сфері.

У літературних джерелах зазначається, що під узагальненим розумінням економічної безпеки може бути використана здатність економічної системи країни (або групи країн) на такий напрямок внутрішнього розвитку та міжнародної економічної взаємозалежності, який буде гарантувати їй (їм) такі умови, які ніяк не будуть загрожувати стабільності економіки та добробуту населення. Т.ч., можна припустити, що економічна безпека нормального функціонування економіки однієї країни безпосередньо залежить від стану порівняльного балансу економік інших країн-партнерів. У зв'язку з цим економічні ризики безпеки, пов'язані з функціонуванням фінансових ринків, є результатом самої природи ринку, який склався.

У сучасному світі, ризики, пов’язані зі стабільністю фінансових ринків, є одними з найбільш важливих показників для економічної безпеки держави. Зрозуміло, що порушення стабільності під впливом заважаючих чинників, загрожує крахом всієї фінансової системи в цілому. У цьому зв’язку концепція безпеки фінансових сфер з методологічної точки зору, вимагає методичного вивчення предмета охорони та дослідження комплексного джерела небезпеки. *Об’єктом охорони*, безсумнівно, є фінансова стабільність та фінансова система в цілому, а *комплексним джерелом небезпеки* на сьогоднішній день є загроза фінансової кризи та особливості системних ризиків. Крім того, не можна не враховувати характерні властивості загроз, які зумовлені відсутністю ефективного інституційного фінансового операційного захисту в області запобігання та врегулювання системних криз.

Запобігання загрозам щодо економічної безпеки, є метою функціонального призначення систем фінансової безпеки, оскільки основним з багатьох чинників, які відносяться до складових економічної безпеки держави, є забезпечення безпеки на фінансовому ринку з точки зору забезпечення добробуту населення.

Глибока трансформація світової економіки веде до зміни форм і принципів функціонування фінансової системи, що викликано, головним чином, глобалізацією фінансових ринків та інтенсивним розвитком технічного прогресу. Масштаби змін, а також їх потужність і, як правило, негативні наслідки, викликані крихкістю та нестійкістю фінансових систем багатьох країн. Крім того, розвиток нових фінансових інструментів, швидкоплинність та розміри короткострокових потоків капіталу, з урахуванням досить нервової реакції учасників ринку на процеси, що відбуваються, зробили середовище функціонування систем фінансової безпеки вкрай нестабільним та невизначеним. В результаті фінансова система стала більш вразливою та чутливою до крахів та криз, що ніяк не сприяє підвищенню загального рівня життя населення.

Фінансові кризи, особливо в дев'яностих роках минулого століття, показали, що вигоди від підвищення ефективності фінансових ринків не є можливими без створення адекватного рівня національної безпеки фінансової системи і, що більш важливо, є нездійсненними з точки зору стабільності міжнародної фінансової системи. Насправді існує свого роду «взаємозамінність» між ефективністю фінансової системи та її стабільністю, що багато в чому визначається ступенем забезпечення безпеки в галузі. Прагнення до високої ефективності може викликати проблеми зі стабільністю, а потім привести до кризи. У той же час обмежувальна політика фінансового забезпечення та надзвичайно суворі заходи щодо забезпечення безпеки можуть викликати зниження ефективності. Т.ч., як показали емпіричні дослідження та припущення, при економічному аналізі та при інших подібних дослідженнях, що стосуються систем фінансової безпеки, все частіше став використовуватися термін «фінансова стабільність» («фінансова стійкість»).

Фінансова стабільність є предметом особливого захисту, який діє в умовах економічного зростання, і, т.ч., інтерес та особливі потреби до нього акцентуються багатьма національними фінансовими системами та світовою економікою в цілому. У цьому сенсі фінансова стабільність вважається суспільним благом, що змушує державні структури до виправданого втручання в процес його захисту. Таке сприйняття фінансової стабільності пояснюється тим, що втрати при кризах (тобто витрати на відновлення фінансової стабільності), несуть всі економічні суб'єкти, включаючи державні структури. Особливо вони позначаються в кінці фінансового року.

Зі сказаного випливає логічний висновок про те, що стан будь-якої фінансової системи, фінансових ринків та забезпечення фінансової стабільності, підлягають правовій охороні в якості суспільного блага.

У науковій літературі представлені різні визначення для фінансової стабільності, але сама концепція ніким ясно не розуміється. Т. Padoa-Schioppa, колишній член Ради Європейського центрального банку, вважає, що фінансовою стабільністю є стан, при якому фінансова система здатна протистояти

шокам до настання зростаючої загрози, яка може негативно впливати на розподіл ресурсів, можливості інвестицій та платежі в економіці. У центральних банках ця функція часто моделюється для підтримки «нормальних умов» у фінансовій системі. Точно так само визначає фінансову стійкість J. Solarz, характеризуючи її як стан динамічного та стійкого балансу взаємопов'язаних фінансових ринків. В принципі, достатньо здоровий глузд говорить про те, що у сенсі суспільного блага, фінансова стабільність в поєднанні зі стабільністю фінансової системи, вказують, що система в цілому не має постійної втрати ліквідності або є неплатоспроможною, фінансові інститути здатні виконувати безперервну діяльність, не мають проблем з виконанням ними своїх зобов'язань і безперервно здійснюють операції наявними фінансовими інструментами. У цьому сенсі соціально значущим станом є підтримка та забезпечення фінансової стабільності основних фінансових інститутів, високий рівень довіри до них як до систем з чіткою та безперебійною роботою, та до таких, які здатні своєчасно виконувати зобов'язання без необхідності зовнішньої фінансової підтримки. Умовою для фінансової стабільності є також стабільність фінансових ринків, можливість проведення довірчих операцій за цінами, які відображають фундаментальні процеси в економіці з урахуванням незначних короткострокових коливань та відсутністю серйозних змін в основних силах, що впливають на ринок.

Стабільність фінансової системи, в свою чергу, визначається як здатність системи до підтримання ліквідності та до підтримки приватних осіб у разі необхідності покриття збитків та ризиків за рахунок власних коштів і, тим самим, як здатність підтримувати платоспроможність.

Під фактором, який забезпечує стабільність, розуміється комплекс у складі «сильної» та «здорової» банківської системи, ринку капіталу та страхового ринку. При цьому враховується, що банківський сектор в більшості фінансових систем світу є домінуючим. Європейський Союз, Сполучені Штати та Японія є трьома провідними світовими гравцями на світових фінансових ринках, який включає їх частку від 20% до 40% в кожній з галузей. Частка Європейського Союзу в світовому банківському ринку є домінуючою і

складає близько 45%. Як показує аналіз літературних джерел, банківський сектор в Україні є найбільшим та найбільш розвинутим сегментом фінансового ринку. Це говорить про те, що банківська система є основою фінансової стабільності в країні.

Як показали недавні фінансові кризи, безгосподарність, що виникла в результаті ескалації банками «поганих кредитів», неналежне та неефективне виконання ними пруденційного нагляду за фінансовим ринком, стали основними причинами банківської кризи [46, 47]. Т.ч., стабільність фінансової системи відноситься, зокрема, і до банківської системи та залежить від двох факторів: інституціональних умов банківської системи та фінансового становища окремих банків. Слід розуміти, що стабільність банківської системи залежить не тільки від діяльності банків в якості незалежних суб'єктів, але й від діяльності установ, які є зовнішніми по відношенню до них. Як правило, зовнішні установи завжди особливо пильні в питаннях стабільності банківської системи. Так, перш за все, особливе місце в системі безпеки вони приділяють банківському нагляду (в сенсі: контролю за фінансовим ринком) та системі страхування вкладів, які за визначенням та своїм функціональним призначенням, є елементами фінансової безпеки.

Враховуючи сказане, під фінансовою стійкістю в цілому можна розуміти стан, при якому фінансова система працює в межах встановлених норм, і без зовнішніх втручань виконує свої функції, що позитивно позначається на загальнонародному добробуті. Слід розуміти, що поняття про фінансову стійкість та про стабільність фінансової системи (стабільність фінансового ринку) багатьма авторами використовуються як взаємозамінні. У цьому сенсі, *перспективами подальших досліджень*, можуть бути питання стабільності фінансової системи при відсутності фінансової кризи, тобто за відсутності системних ризиків. Крім того, варті уваги питання стабільності фінансової системи з урахуванням проблем окремих фінансових інститутів та сегментів фінансового ринку, а також їх вплив на функціонування фінансової системи в цілому.

2.5. Аналіз аномалій мережевого трафіку інформаційно-обчислювальних систем спеціального використання

Зі збільшенням використання різних типів трафіку, як в корпоративних мережах, включаючи банківські структури, так і в мережах провайдерів зв'язку, мережеві оператори вимушені здійснювати моніторинг властивостей трафіку щоб підвищити віддачу від інвестицій, підтримувати рівень сервісу і захистити мережеві ресурси. На основі аналізу та обробки даних, які отримуються від спеціальних модулів контролю трафіку, необхідно формувати цілісну картину роботи мережі у вигляді логічної схеми стану контрольованих об'єктів. Для цього заздалегідь оброблену інформацію необхідно передавати для зберігання й подальшої обробки на спеціалізовані сервери – *CDR* (*сервери детальної реєстрації викликів*) і сервери Frod-менеджменту – *FMS*. При цьому доступ до спеціалізованих додатків системи повинен забезпечуватися через робочі місця операторів дружніми інтерфейсами.

Огляд наукової літератури, яка присвячена проблемам аналізу мережевого трафіку в банківських структурах (наприклад, [48…51] та ін.), показав, що для ринку телекомунікаційних послуг в даний час характерний вельми специфічний стан. На жаль, нові технології аналізу трафіку стали використовуватися в рамках різних махінацій. Наприклад, більше половини трафіку ВАТ «Укртелеком» в даний час відноситься до категорії *безконтрольного*. Як правило, це відбувається в результаті того, що оператори недобросовісних компаній використовують різні схеми для приховання результатів свого реального трафіку. Причини цього достатньо специфічні і не розглядаються в рамках даного дослідження.

Українська мережа обміну Інтернет-трафіком (*UA-IX*) є членом Euro-IX – Міжнародної Асоціації, яка об'єднує сорок мереж обміну трафіком, розташованих в 23 країнах світу, з метою розвитку, зміцнення і удосконалення співтовариства точок обміну трафіком (*IXP*) між банками та іншими структурами. Створення *спеціалізованої мережі*, яка контролює дані про обмін трафіком, дало можливість учасникам значно скоротити витрати і розширити

можливості банків, а також малого бізнесу. Маючи дві точки обміну Інтернет-трафіком, вказана мережа є заставою стабільності Інтернет-ринку України. За своїм обсягом, значущістю і сферою діяльності мережа є унікальним підприємством України. У мережі присутній спеціалізований сервер, який забезпечує надання інформації про поточний стан мережі обміну трафіком (*Looking Glass*), а також інформацію про об'єми трафіку, що проходить через мережу. Т.ч., з урахуванням сказаного, отримання даних про статистичні властивості трафіку, включаючи банківські та інші фінансові структури, а також експорт із загального масиву необхідних даних для подальшого використання, визначає актуальність питання, винесеного в заголовок підрозділу. Метою роботи, виконаної у даному підрозділі, є виявлення аномалій мережевого трафіку між банками для підтримки необхідного рівня сервісу і захисту мережевих ресурсів. При цьому враховується, що порушення цілісності інформації або перехоплення в мережі, в поточному контексті, є *аномалією*.

Сформулюємо завдання в загальному вигляді. Завдання аналізу трафіку з метою виявлення та врахування його аномалій полягає в знаходженні компромісу між інтервалом спостереження і детальністю опису. Такий підхід можливий тільки при детальному вивченні природи трафіку і топології мережі. У ідеалі і, отже, кінцевою метою рішення задачі, може бути синтез методу перетворення топології мережі з урахуванням ефектів агрегації для забезпечення можливості проведення експериментів перевірці валідності всіляких теоретичних методів оцінки магістрального трафіку. Базуючись на цьому, перейдемо до викладу основного матеріалу.

Технології моніторингу і виявлення аномалій розділяються за джерелами і типами даних, механізмами виявлення і часу реагування. Аномалії в поведінці трафіку визначають характер збоїв в мережі, якими можуть бути, наприклад, необґрунтоване зростання або падіння інтенсивності трафіку, зміни в стаціонарному характері трафіку, надмірне підвищення інтенсивності використання окремих частин мережі і т.д. Як правило, це свідчить або про ненадійну роботу апаратур-

ної частини, або про зовнішні втручання (зокрема – атаки на мережеві ресурси, що ведуть до різкого необґрунтованого збільшення трафіку).

Виявлення і розпізнавання аномальної поведінки мережі адміністраторами часто ґрунтується на методах, відомих як «ad hoc», тобто на методах спеціальних, суб'єктивних, таких, що з'явилися в процесі довготривалої роботи у області управління мережею.

Аномалії у зв'язку зі збоєм апаратно-програмного забезпечення вельми характерні в умовах, коли матеріальна база створюється в обмежених фінансових можливостях. Дана ситуація типова для сучасного ринку телекомунікаційних послуг, які надаються фінансовим струтурам в Україні. На рис. 2.1 відображений приклад таких аномалій для спостережуваного трафіку з п'ятихвилинним усереднюванням.

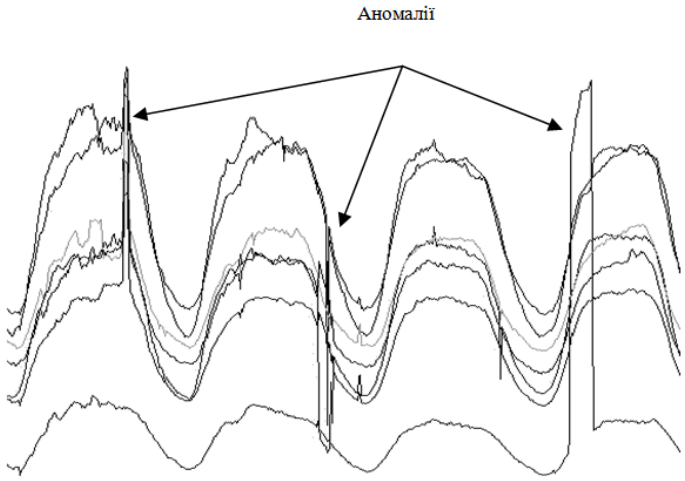


Рис. 2.1. Аномалії трафіку міжнародного покриття Українським сегментом мережі при апаратних відмовах у фінансових структурах

Слешдот-аномалія (*Slashdot* або *Flash crowds*) – аномалія, яка, по суті, є могутнім сплеском відвідуваної ресурсу мережі, після того, наприклад, як посилання на цей ресурс з'являлося на стрічці новин популярного мережевого видання або блога. Термін і саме явище з'явилися завдяки популярному інформаційному технологічному блогу *Slashdot*. Саме тоді була вперше відмічена дана аномалія, яка на сьогоднішній день часто виявляється. Для даного ефекту є характерним те, що гігантське збільшення трафіку наростає стрімко, фактично перетворюючись на *DDoS*-атаку, так що сайт, який не розра-

хований на таку кількість відвідувачів, дуже швидко стає недоступним або доступ до нього стає надзвичайно важким через перевантаженість сервера або недостатньої пропускної спроможності каналів зв'язку (рис. 2.2). Слешдот-ефект володіє такою руйнівною силою через часовий чинник, тобто через різку зміни стану мережі в короткий часовий дискрет.

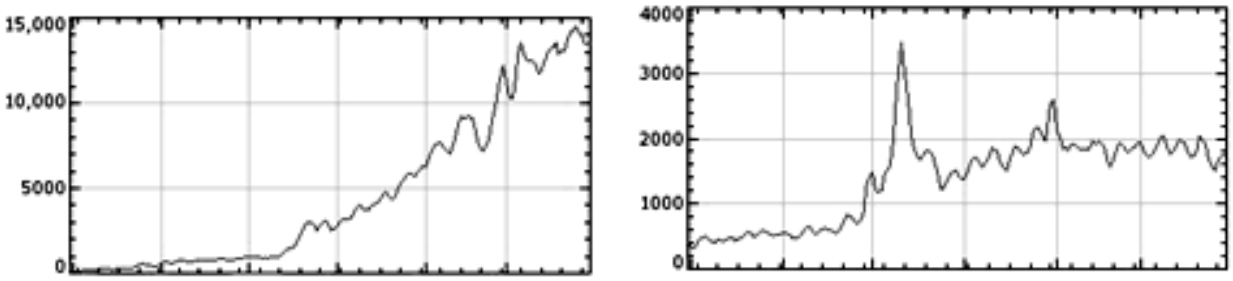


Рис. 2.2. Слешот-аномалія

Як показали практичні спостереження, проведені впродовж останнього року, найчастіше аномалії виникають в результаті різних атак. Наприклад, встановлено, що так звана *DoS/DDoS-атака* переслідує своєю метою вивести об'єкт з робочого стану. Звичайно, в більшості випадків глобальна атака приводить до великих фінансових втрат того суб'єкта, який атакується. Наприклад, якщо який-небудь комерційний сайт стає недоступним на декілька годин, то це завдасть шкоди бізнесу, а якщо на тиждень, то наслідки можуть бути ще більш катастрофічними.

Аналогічна ситуація характерна і для локальних мереж. Річ у тому, що одним з ефектів популярних атак DoS (*Denial of Service*), є величезний трафік, що направляється на жертву. Якщо для великої фірми це не такий важливий інцидент, якому варто приділяти першорядну увагу, то для невеликого підприємства навіть середня атака може загрожувати розоренням. Окрім величезної шкоди, що наноситься жертві, такі напади відрізняються простотою і величезною ефективністю. Проти них немає стовідсоткового захисту.

Атаки *TCP SYN Flood* і *TCP-flood*, які відносяться до того ж класу блокування роботи мережі, переслідують метою перевищити обмеження на кіль-

кість з’єднань, які знаходяться в стані установки. Як показав аналіз, вони організовуються на базі комп’ютерних вірусів. На рис. 2.3 відображений приклад аномального трафіку в результаті *TCP-flood*-атаки, проведеної на базі впровадження вірусу.

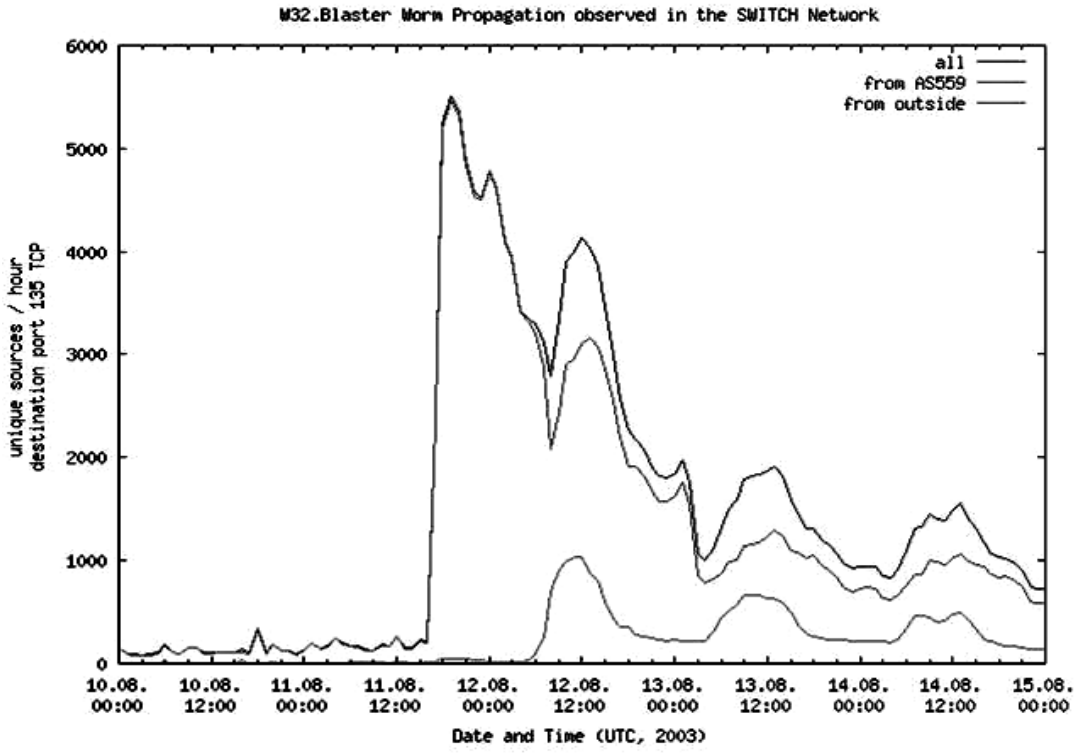


Рис. 2.3. Трафік в період розповсюдження вірусу в мережі

Практичні роботи показали, що аномальний трафік спостерігається при виникненні ситуації нестабільності маршрутів, коли маршрутизатор з високою частотою анонсує маршрут в певну мережу через різні маршрутизатори призначення чи ж чергує анонси відповідними анонсами про недоступність даної мережі.

Близька ситуація – нестабільність мережевого інтерфейсу. Наприклад, унаслідок апаратного збою пристрій поперемінно визначає стан свого мережевого інтерфейсу як «робочий», «не робочий». До нестабільності маршруту приводять аварії в мережі, викликані апаратними або програмними збоями, випадковими помилками на лініях зв’язку, ненадійними з’єднаннями і т.д.,

що в свою чергу призводить до того, що частина маршрутної інформації пропадає і з’являється знову (рис. 2.4).

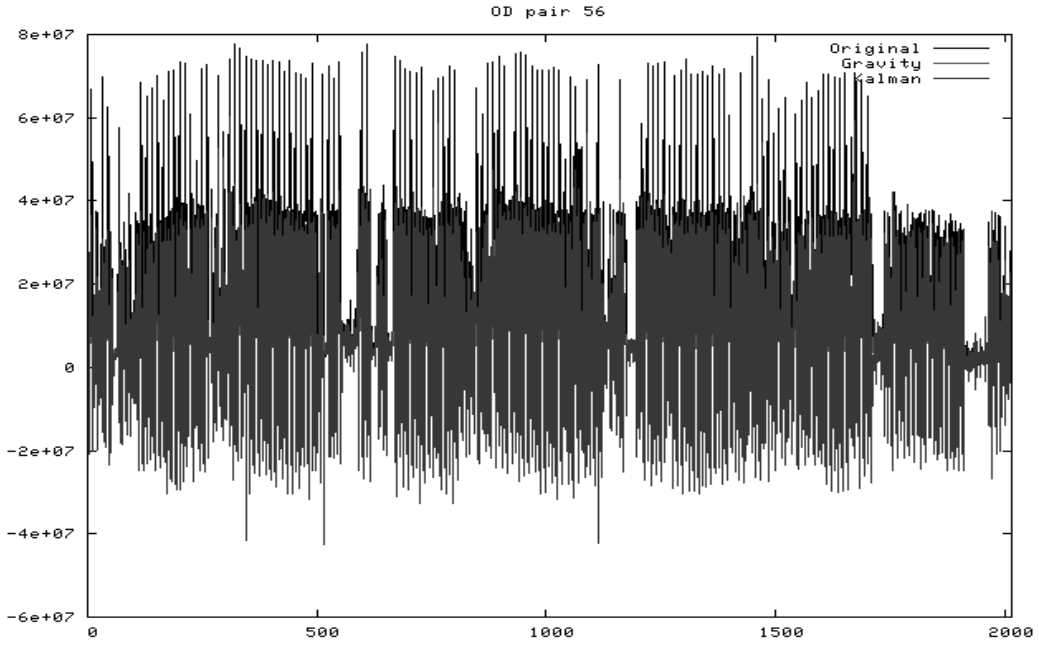


Рис. 2.4. Аномалії трафіку при нестабільності маршрутів

У мережах, де для побудови таблиць маршрутизації використовується протокол, в основі якого лежить протокол маршрутизації стану каналу (*link-state*), нестабільність маршрутів приводить до частого перерахунку топології всіма маршрутизаторам в одному домені маршрутизації. У мережах з дистанційно-векторними (*distance vector*) протоколами маршрутизації, нестабільність маршрутів спричиняє за собою часту розсилку повідомлень про зміну маршрутів. У обох випадках це перешкоджає збіжності мережі, тобто стану, в якому всі маршрутизатори використовують однакове розуміння маршрутизаторами поточної мережевої топології. Після порушення збіжності потрібен час для того, щоб маршрутизатори обмінялися інформацією для відновлення збіжності нової мережевої топології.

Відзначимо, що для умов економіки, що розвивається, можливо наявність аномального трафіку через різні зовнішні причини: силове обмеження потоків, внесення пріоритетності, дія різних політичних подій, указів і т.д.

Часто ці аномалії вимагають детальнішої інформації для пояснення. Приклад їх приведений на рис. 2.5.

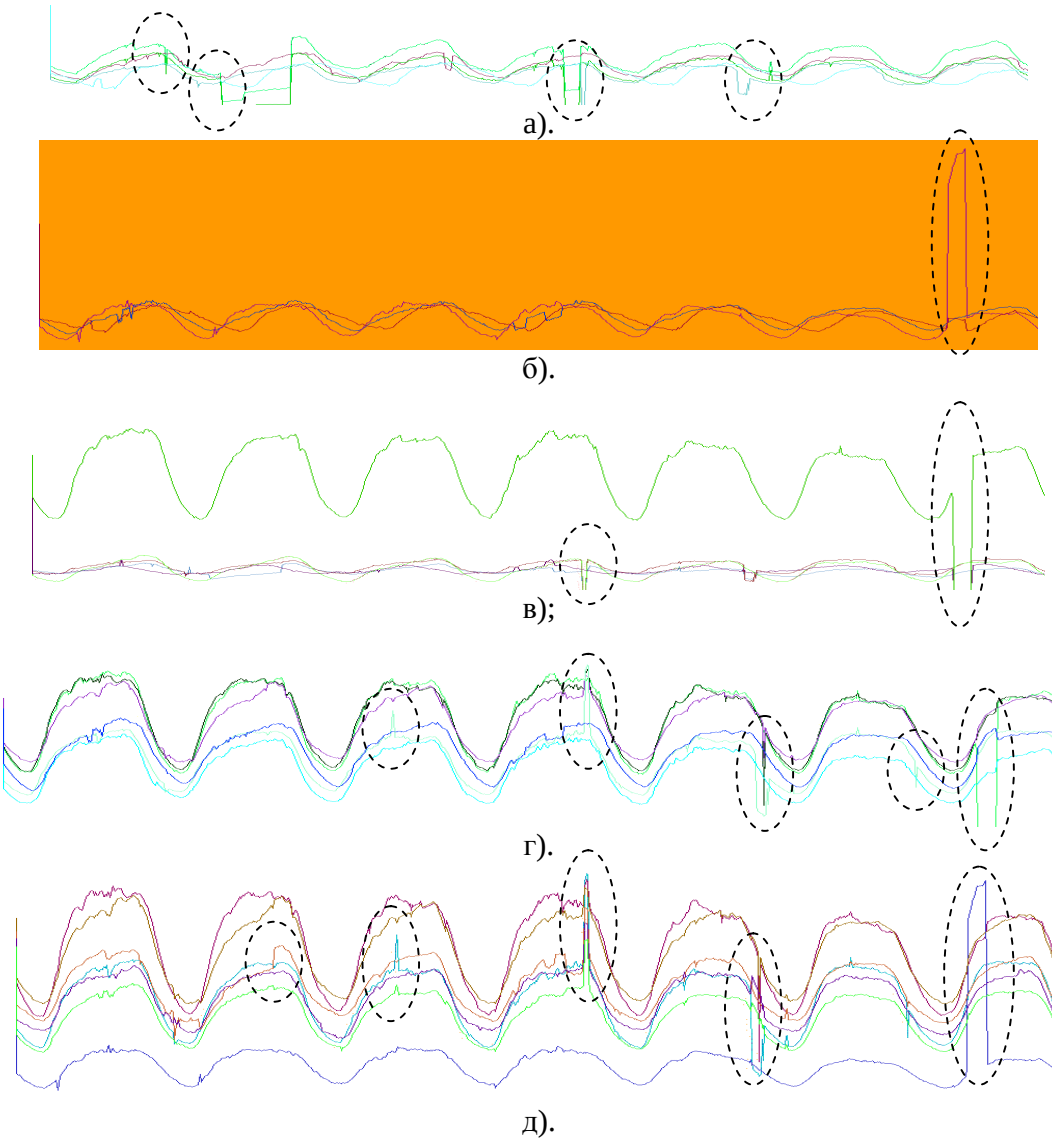


Рис. 2.5. Приклади аномалій трафіку, що вимагають додаткових досліджень

Важливим моментом при розробці моделей дослідження або моделювання трафіку, є отримання інформації щодо використання Wi-Fi-технологій в комплексних системах телекомунікацій [52, 53], які використовуються фінансовими підприємствами. На сьогодні, в умовах економічної кризи, Wi-Fi по праву може вважатися однією з найбільш перспективних технологій в Інтернет-індустрії, зручній у використанні і оптимальній по співвідношенню «ціна-якість». Стандарт Wi-Fi дозволяє фінансовим установам надавати ви-

сокошвидкісний доступ до всіх ресурсів мережі Інтернет, як своїм корпоративним клієнтам, так і власникам ноутбуків і кишенькових комп'ютерів. У зоні покриття мережі Wi-Fi можливо підключення будь-якого пристрою, оснащеного відповідним модулем, що підтримує стандарт IEEE 802.11. Технологія забезпечує одночасну роботу в мережі декількох десятків активних користувачів. Швидкість передачі інформації для кінцевого абонента може досягати 54 Мбіт/с. Пропускна спроможність стандарту може бути порівняна з пропускною спроможністю високошвидкісної виділеної лінії. У містах з історичними пам'ятниками, де прокладка кабелів особливо скрутна, перевага такого підходячи очевидно. Але, як показали спостереження, мінуси все ж таки є. Так, число випадкових чинників при використанні радіоканалу істотно зростає, що спричиняє за собою ще більш стохастичний характер трафіку (рис. 2.6).

Характерно, що в мережевому трафіку Wi-Fi спостерігаються періодичні провали як при передачі даних від маршрутизатора до бездротового адаптера, так і у зворотному напрямі. Швидкість передачі даних між двома бездротовими адаптерами може впасти по безлічі причин. Іноді виникають ситуації, коли неможливо встановити з'єднання. Отже, дослідження статистичних закономірностей трафіку Wi-Fi-мереж, є перспективною проблемою *подальших досліджень* стосовно питань аналізу трафіку.

Як видно з наведених матеріалів, в результаті аналізу окремих аномалій мережевого трафіку в магістральних банківських каналах зв'язку показано, що обробка статистичних даних мережевого трафіку може бути основою для організації їх експорту з загального масиву для зовнішніх додатків і проводити облік аномалій для підвищення якості сервісу, що надається, і організації захисту даних. При аналізі виявлені аномалії мережевого трафіку, облік яких необхідний при моделюванні роботи всіляких мережевих додатків.

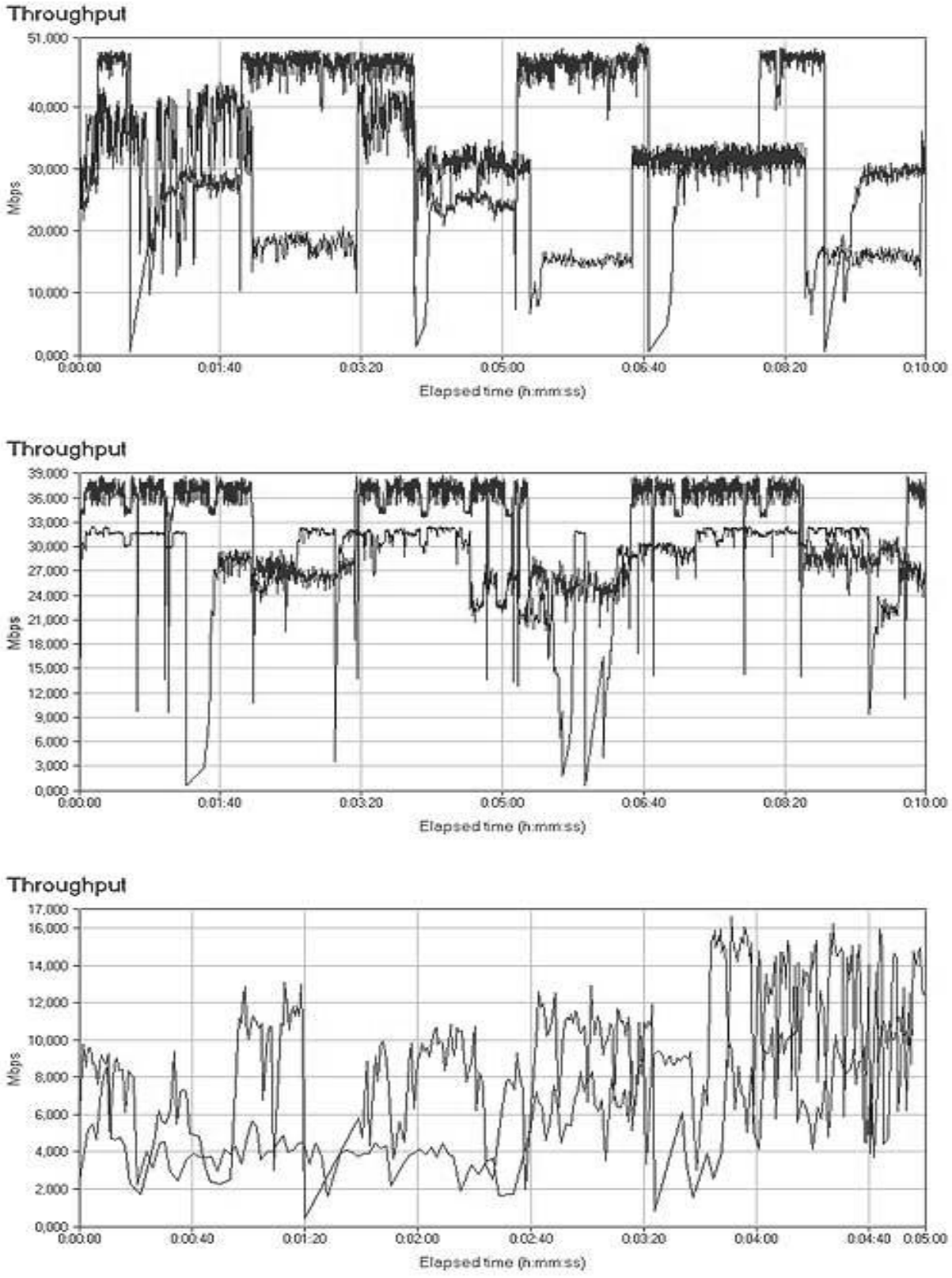


Рис. 2.6. Непряме відображення трафіку пари «Відправник-Отримувач» при використанні Wi-Fi технології

2.6. Принципи побудови захищених мереж сфери економіки, бізнесу та фінансів

Принципи побудови захищеної мережі у сфері економіки, бізнесу та фінансів (ЗМ) визначаються її призначенням, концепцією, функціями, соціально-фінансовою базою, фізичною і економічною географією, топографією і демографією країни [54].

За визначенням принцип (лат. *principum – початок, основа*) – основне початкове положення, основна особливість. Ведучим, визначальним принципом побудови ЗМ є соціальна спрямованість, що задовольняє соціальну необхідність для суспільства, яке розвивається. Змістовне наповнення основного принципу є ситуаційним та регіональним. Воно визначається ступенем задоволення суспільних (владних, ділових, індивідуальних) потреб при допустимому ресурсно-фінансовому навантаженні. Поєднання соціальної спрямованості зі складністю породжує специфічні колізії внутрішнього характеру.

В зв’язку з цим невирішеною проблемою стосовно захищених інтелектуальних мереж сфери економіки, бізнесу та фінансів, є встановлення концептуальної основи принципів побудови та функціонування ЗМ, яка диференціюється на компоненти – конкретні принципи побудови як самої технічної системи в цілому, так і її окремих компонентів [55].

Результати аналізу досліджень та публікацій з відповідними посиланнями та висновками, викладені по змісту підрозділу. В подальшому під ЗМ будемо розуміти ЗМ сфери економіки, бізнесу та фінансів, а також інших галузей, які споріднені з ними.

Принцип спадкоємності. Звичайно на території будь-якої країни діють декілька напівавтономних ЗМ традиційних видів зв’язку: державна, відомчі, загальногромадська. Разова заміна сукупності або окремих сегментів цих мереж на ЗМ неможлива. Неможливо і перетворення діючих відомчих або виділених мереж в ЗМ. Принцип спадкоємності полягає в створенні ЗМ, які діятимуть одночасно з існуючими інформаційними мережами з поступовою пе-

редачею їм функцій і послуг та елімінуванням компонентів існуючих мереж або раціональним одночасним включенням їх компонентів в ЗМ [56].

Одночасне введення в дію всіх компонентів окремих ЗМ не повинне створювати психічного дискомфорту і негайного відходу від динамічних стереотипів.

Спадкоємність повинна дотримуватися і в системі оплати послуг, у всій комерційній діяльності. Існуюча тарифікація послуг інформаційних і телекомунікаційних мереж нездійснена, неефективна: вона не відповідає інтересам ні користувача, ні власника мережі. Проте – вона звична, а її зміна викликає неприйняття користувачів і персоналу мережі. Найнеперспективніше і безрозсудне – стрибкоподібна зміна тарифів, непідготовлена і недостатньо обґрунтована. Навіть введення нових, найпрестижніших і корисніших послуг не повинне супроводжуватися різким фінансовим тиском. Аналогічним чином справа йде з пріоритетами і пільгами [57].

В цілому фінансова політика ЗМ повинна носити еволюційний характер. Принцип спадкоємності повинен дотримуватися у всіх сферах діяльності по створенню, експлуатації і розвитку ЗМ.

Принцип перспективності. ЗМ повинна бути перспективною в технічному, соціальному, фінансовому відношенні. Поняття перспективності не має чіткої і однозначної дефініції, вимагає футурологічного обґрунтування. Те, що на перший погляд здається непотрібним, може насправді виявитися перспективним, і навпаки. За визначенням перспектива (лат: *perspisio – ясно бачу*) – плани, плани на майбутнє. Трудність полягає в раціональній оцінці цих планів. Варіанти планів розрізняються:

1) етапністю застосування різних технічних засобів і технологій їх створення;

2) системами пріоритетів і тарифів;

3) порядком впровадження нових типів послуг;

4) методами і рівнем автоматизації управління і т.д.

Оцінка перспективності вимагає аналізу ситуації, її прогнозування і кількісного порівняння альтернатив [58]. Крім методів наукової футурології

(розроблених далеко не достатньо) можна використовувати передовий досвід розвинених країн. На жаль, національні традиція явно не прогностична: значна (якщо не більша) частина світових досягнень має або російський, або український генезис, проте по широкому впровадженню нових ідей ці країни чомусь завжди позаду. Ця сумна обставина повинна насторожувати, проте викорінювання шкідливої традиції не повинне супроводжуватися необґрунтованою ейфорією до будь-якої новизни.

Принципи прибутковості. ЗМ є комерційною системою. Її дохід (навіть у тій галузі, яка є предметом дослідження у цьому підрозділі) повинен перевищувати витрати (експлуатація плюс розвиток). Оскільки мають місце капітальні витрати, здійснити це непросто, особливо якщо йдеться про короткі терміни. На першому етапі необхідні кредити та інвестиції. На подальших етапах кредитування не виключене, принаймні для деяких операцій, пов’язаних з великими витратами (закупівля комплектуючих частин, термінові будівельні роботи, монтаж крупних об’єктів). Враховуючи, що кредити навіть на короткий термін видаються під значні відсотки, необхідно забезпечити швидку віддачу від вкладень. Досягти цього можна за допомогою раціональної стратегії і гнучкої тактики вибору користувачів, високої соціальної значущості упроваджуваних компонентів системи.

Абонентам і клієнтам необхідно не тільки показати «товар лицем», не тільки сформувати про ЗІС добру думку, але й наполегливо пропагувати її корисність як тимчасової безкоштовної (низькооплачуваної) клієнтської та абонентської мережі з підвищеною надійністю щодо захисту інформаційних ресурсів. Цей прийом, як показує практика, діє безвідмовно і стійко. Створюється нове підприємство (установа), нова комерційна структура, організовується банк. Компанія (корпорація), що створює і експлуатує ЗМ, пропонує встановити устаткування з невисокою оплатою (для проби) на певний термін. Після закінчення терміну або користувачі починають оплачувати послуги (включаючи установку) з високого тарифу, або апаратура відключається. До виключення справа, зазвичай, не доходить: від звичних і ефективних послуг

важко відмовитися. Зрозуміло, така тактика буде ефективною тільки при високій корисності послуг і прибутковості експлуатації. Враховуючи, що створення ЗМ припадає на період стійкої інфляції і неконвертованості національної валюти, комерційна стратегія і тактика повинні формуватися з урахуванням цієї обставини: інфляція стимулює мінімальні терміни використання кредитів [59].

Ще один чинник прибутковості – акціонування ЗМ. Оскільки акціонери зацікавлені в дивідендах, вони можуть зробити багато що для підвищення рентабельності ЗМ, зокрема вкладати гроші в розвиток через покупку акцій. Акціонери-підприємства не так вже зацікавлені в швидкій віддачі вкладень: їх більше цікавлять послуги, які можна одержати в короткий термін. Вслід за підприємствами і відомствами потягнуться індивідуальні акціонери для яких привабливістю є стійкість дивідендів. У цьому сенсі ЗМ – один з найбільш надійних партнерів, оскільки вона необхідна суспільству і не може збанкрутіти. Частина зарплати співробітникам може виплачуватися акціями: це допомагає оптимізувати фонд зарплати і стимулює старанність персоналу, який матиме подвійну зацікавленість: дивіденди/заробіток. У цих умовах додатковий контингент акціонерів буде безперервно розширюватися за рахунок значної частини населення, зацікавленої в придбанні та розширенні послуг.

Принцип прибутковості не може бути безпосереднім критерієм для оцінки діяльності ЗІС, оскільки на прибуток мають достатньо високий вплив зовнішні умови. Так, зокрема, пільгове оподаткування може істотно підвищити прибутковість, а прогресивне – взагалі знищити прибуток. Але як оперативний показник розглянутий принцип є ведучим.

Принцип синергетичності. Будь-яка система може існувати і діяти тривалий час у формі однієї з трьох організаційних структур:

1) жорсткого силового програмного управління структурою та функціями;

2) самоорганізації (тобто синергетичності);

3) у змішаній формі.

Синергетичність направлена на внутрішню структуризацію ЗМ: переорі-

єнтацію її так, щоб сприяти підвищенню ефективності системи (не зменшуючи здібності до самозбереження).

У складних ЗМ може спостерігатися безперервне протистояння тенденції підвищення неупорядочності, хаотичності, дезорганізації і тенденції утворення високовпорядкованої структури. У ЗМ структура схильна до стохастизму (в першу чергу зважаючи на саму структуру побудови інформаційної мережі, яка визначає випадковість пошуку з'єднання через декілька комутаційних пунктів при великому навантаженні), спорадичного наростання викликів і можливої зайнятості ліній. Ліквідовувати стохастизм за допомогою управління іноді неможливо, оскільки розібратися в наявній схемі з'єднань при наростаючому числі незадоволених вимог не вдається: зміна ситуації відбувається швидше і, крім того, неминуче запізнювання реакції. Набагато простіше, виявляється, не допустити стохастизм (точніше, квазистохастизм), ніж усунути його: навіть невелика плутанина в з'єднаннях (подібну плутанину ми спостерігаємо щодня, коли телефонна мережа сполучає нас з випадковим, а не з викликаним абонентом) є зародком квазистохастизму, який, сформувавшись, має тенденцію до наростання.

Навіть одне неправильне з'єднання або роз'єднання абонентів ЗМ, не замовлене групове з'єднання, непроходження виклику, помилковий виклик і т.д. вносять істотний розлад в роботу захищеної мережі. В ЗМ, які досягли деякого рівня складності (хоча б із-за збільшення числа абонентів і комутаційних вузлів), розлад може стати стійким та непрогнозованим і переходити в квазистохастизм [60].

Самоорганізація діє як внутрішній регулятор порядку та організації. Раціональна синергетика пов'язана або з випереджаючою (прогностичною) реакцією на квазистохастизм, або з малою реакцією, що запізнюється (реакція повинна затримуватися на якийсь час, який є меншим періоду кореляції стохастичного процесу).

Принцип синергетичності полягає в швидкій «виправляючій» реакції на прояв зародка квазистохастизму структурно-програмними засобами.

Гіперсинергетика в будь-якій системі обслуговування (до яких відносяться ЗМ) не менш небезпечна, ніж квазистохастизм. Підвищена і невиправдана схильність до самоорганізації виражається перш за все в стабілізації типу помилок і виникненні «організованих» помилкових викликів. Гіперсинергетика може виникнути при стійкій помилці реакції (достатньо на протязі деякого часу постійно плутати між собою дві цифри в наборі коду абонентів, що може відбутися унаслідок несправності) або, навпаки, при стійкому надмірному запізнюванні (гальмівна синергетика). Усувається гіперсинергетика регулюванням. Основна трудність при цьому полягає в діагностиці того пристрою (програми, методу, системи), який потрібно регулювати.

Нестійкість ЗМ виявляється в окремих просторово-часових зонах. Нестійкість, що викликається змінами зовнішніх параметрів системи, приводить врешті-решт до утворення нової динамічної просторово-часової структури. Виникають і встановлюються параметри порядку, слідством чого є зменшення числа мір свободи: наступає «поточна рівновага». Оскільки синергетика пов’язує динамічні і стохастичні процеси, ця рівновага носить специфічний характер і може виразитися в наростанні або динаміки порядку, або стохастизму під впливом зовнішніх чинників – користувачів і управління.

Принцип керованості. Підсистема управління в ЗМ виконує функцію контролю і формування цілеспрямованості. Контроль повинен бути таким, що передбачає, щоб вчасно попередити розладнання. Цілеспрямованість підтримується для забезпечення максимального задоволення потреб контингенту користувачів [58, 59, 64].

В управлінні ЗМ можуть використовуватися різні механізми:

– програмний і ситуаційний – для забезпечення технічної надійності;

– ситуаційний і адаптивний – для забезпечення функціональної діяльності;

– адаптивний і рефлекторний – для управління споживачами.

Одночасно діють декілька видів управління, взаємозв’язаних між собою, але які використовують різні механізми і засоби дії на об’єкти управління.

Слід розрізняти:

– технічне управління – для попередження і усунення відмов апаратури й устаткування, підтримка ЗМ в безперервній готовності до дії;

– функціональне управління – для підтримки й узгодження робочих функцій, стимулювання працездатності, захисту від квазистохастизму та гіперсинергетики;

– оперативне управління – для забезпечення високої якості обслуговування та раціональної ситуаційної реакції;

– адміністративне управління – для попередження й гасіння внутрішніх конфліктів, забезпечення високої продуктивності праці, безперервного підвищення рівня організації;

– управління розробками – для висунення нових ідей, їх технічного та організаційного втілення, оцінки результатів;

– управління розвитком – для екстенсивного та інтенсивного розвитку ЗМ, збільшення контингенту користувачів та складу послуг, просторово-часового розширення.

Перераховані види управління взаємозалежні та взаємопроникні [61, 63]. У сукупності останні три види управління входять в координаційне управління.

Принцип інформативності. Принцип інформативності ЗМ полягає у випередженні попиту та спирається на:

1) створення захищених широкосмугових каналів;

2) максимальне використання інформаційної ємності;

3) оптимальний розподіл інформації в часі та просторі;

4) рівномірне завантаження ЗМ.

Заміна устаткування в ЗМ обходиться набагато дорожче за стратегію попереджуючої інформативності. Наявність інформаційного резерву дозволяє швидко привертати та освоювати нові контингенти користувачів і розширювати діапазон послуг.

При підключенні до ЗМ нових територій можна йти двома шляхами:

– нарощувати систему;

– створювати канали нових типів.

Мабуть, доцільно використовувати обидва шляхи, але другий є переважнішим, не дивлячись на тимчасове недовантаження.

Максимальне використання інформаційної місткості ЗМ, може здійснюватися шляхами:

1) оптимізації схеми з'єднань між комутаційними пунктами;

2) раціонального використання багатоканальних ліній;

3) застосування пристроїв інтеграції та диференціації каналів.

Найбільше навантаження несуть сполучні лінії ЗМ, тому необхідно забезпечити гнучкість комутації у разі пікового навантаження. Гнучка комутація виручає також при виході з ладу різних компонентів ЗМ, при виведенні частин ЗМ на профілактику і в надзвичайних ситуаціях. Оскільки інформативність ліній різних типів не однакова, необхідно раціонально використовувати багатоканальні лінії з тим, щоб компенсувати недостатню пропускну спроможність інших ділянок ЗМ.

Оптимальний розподіл інформації в часі і просторі враховує поточне завантаження ЗМ, потік вимог на послуги, оцінку терміновості замовлень, встановлені пріоритети і тарифи. Потік вимог, що поступають від всієї розгалуженої мережі абонентів і клієнтів, раціонально спочатку фільтрувати: надстрокові, термінові, такі, які можна виконати протягом хвилин, годин, доби: чим менша терміновість, тим нижчий тариф – абоненти це враховують; конфіденційні переговори, повідомлення, передача документів з грифами секретності, запити до закритих інформаційних ресурсів; передбачувана тривалість послуги; необхідна смуга пропускання і т.д. На перший погляд – дуже великий набір ознак, які потрібно врахувати. Проте за наявності апріорної класифікації фільтрація представляється не таким вже складним завданням в якому велика частина навантаження лягає на абонента: саме він в першу чергу вирішує, яка йому потрібні терміновість і рівень захищеності та скільки

він готовий платити за конкретні послуги. Виключення допустимі для надзвичайних ситуацій, в яких оптимізація не обов'язкова [62].

Рівномірність завантаження ЗМ досягається за допомогою введення в систему буферної пам'яті на захищених комутаційних вузлах, в першу чергу в телепортах, де накопичуються нетермінові замовлення на послуги, які не пов'язані з оперативністю. Це декілька ускладнює склад вузлового устаткування, але зменшує тиск на лінійну частину, яка найбільш консервативна і важче нарощується. Відповідно вибираються – виходячи з умови рівномірності навантаження – сполучні траси. При структурі подвійного моноканалу це досягається достатньо легко.

Принцип розвитку. Це провідний і дуже загальний принцип: *ЗМ повинна розвиватися територіально і технічно разом з соціумом, а враховуючи терміни створення системи – швидше за соціум*. Принаймні 8...10 років (в кращому разі) буде потрібно, щоб забезпечити послугами соціум регіону, що вже сформувався, але за цей час чисельність населення в регіоні збільшиться.

Технічний розвиток ЗМ повинен бути випереджаючим. Наприклад, вже є близькою до ідеальної реалізації нова модель телефонного апарату з дуже великими можливостями, яка відома під назвою «персональний коммуникатор». Цей апарат малий по габаритах, суміщає функції електронного записника, телефаксу, телефону стільникового зв'язку, дозволяє зв'язатися з персональним комп'ютером і підключитися до інформаційної системи (у тому числі і ЗМ) в будь-якому пункті. У нього типовий, відповідний стандартам і широко використовувана різними інофірмами мова зв'язку. Враховуючи, що вітчизняний ринок (ще й з урахуванням ближнього зарубіжжя) неосяжний, то упровадивши в апарат функції захисту інформації, можна розраховувати на великий об'єм замовлень, соціальний і комерційний успіх.

Що стосується споруди ЗМ, її поетапного введення, експлуатації і управління, то все повинно виконуватися вітчизняними силами. Це створює ще й велику кількість нових робочих місць, притому кваліфікованих.

Принцип етапності. Принцип етапності ЗМ визначає її просторово-часову зміну і розвиток як технічної системи, її статус в кожен момент часу. Очевидно, необхідно створити ЗМ так, щоб можна було в певний момент «включити» її відразу всю цілком, неможливо навіть теоретично. Це суперечить основному (соціальному) принципу і принципам прибутковості та розвитку. ЗМ повинна створюватися і вводитися в дію поетапно.

Відповідно до основного принципу та вітчизняних реалій доцільно передбачити [64]:

– створення виділених ЗМ ділового призначення;

– перехід від виділених систем до накладених;

– зрощення ЗМ з існуючою інформаційною мережею;

– створення єдиної (інтегрованої) захищеної телекомунікаційної мережі загального призначення.

Зміна етапів може бути регіональною, навіть субрегіональною. По суті, на території країни практично діятимуть всі етапи одночасно, але в різних місцях. Це не перешкоджає гармонійному еволюційному розвитку ЗМ і раціональній технічній експлуатації, навпаки, стимулює їх завдяки спадкоємності досвіду випереджаючих частин і структур системи [65].

Принцип екологічності. Навколоземний і космічний простір насичений електромагнітним випромінюванням – від жорстких гамма-променів до наддовгих хвиль. Природні електромагнітні поля благотворно впливають на життєдіяльність – в електромагнітному океані зародилося і еволюціонувало життя. У живому організмі відбуваються різні природні електромагнітні процеси – на субклітинному, клітинному, органічному, підсистемному, загальносистемному, екологічному рівнях.

Власні електромагнітні поля живого складаються з зовнішніми полями, утворюючи складну динамічну структуру електромагнітної взаємодії живої істоти з навколишнім середовищем. Топологія результуючого електромагнітного поля (ЕМП) надзвичайно тонка і складна, її структура змінюється на нанометрових і ангстремних відстанях, вона набагато тонша, ніж структура

речовини в організмі. Електромагнітні поля істотно впливають на фізіологічні процеси. Природні ЕМП діють гармонійно: їх вплив, починаючи з субклітинного до екологічного рівня, фізіологічно однонаправлені та виправдані з погляду виживання і адаптації до середовища.

Дія штучних ЕМП, породжених технічними засобами, зокрема засобами ЗМ, може бути альтернативною на різних рівнях живого і викликати фізіологічну дисгармонію самих різних напрямів. Зараз ця проблема виходить на передній план. Наприклад, зважаючи на близькість абонентського радіотелефону до головного мозку зафіксовано збільшення онкологічних захворювань на 6...8% у користувачів радіотелефоном (не дивлячись на його мізерну потужність) в порівнянні з середнім рівнем.

Принцип ефективності. ЗМ повинна бути ефективною на всьому життєвому циклі. Це провідний чинник технічного, наукового і соціального розвитку.

На підставі цього принципу повинна формуватися стратегія розвитку ЗМ, операторська діяльність, комерційна політика, інвестиційно-кредитна політика, внутрішня соціальна політика, нарешті – вся технічна політика [66].

Принцип ефективності ЗМ тісно стикується з основним (соціальним) принципом і забезпечує його функціонально [67]. Він визначає і вінчає ідеологію та концепцію ЗМ.

Як слідує з вище зазначеного, концептуальний генезис викладених принципів очевидний. Принцип спадкоємності забезпечує як технічний розвиток, так і швидке освоєння системи користувачами; принцип перспективності – тривалий життєвий цикл системи, отже, її прибутковість. Принцип розвитку визначає відповідність системи загальному рівню техносфери й суспільства. Принцип екологічності пов’язаний зі станом здоров’я і рівнем життя соціуму. Принцип інформативності визначає вплив системи на к.к.д. особистої та суспільної праці. Принцип прибутковості безпосередньо визначає прибутковість системи. Мінімізація часу адаптації досягається за рахунок принципу синергетичності, а захист від непрогнозованих дій і процесів – принципу керованості. Принцип етапності забезпечує реалістичність концепції. Принцип ефективності зв’язує воєдино соціально-економічну і технічну концепції.

Висновки до розділу 2

Встановлено, що до показників економічної безпеки відносяться наступні:

– показник економічного зростання: динаміка і структура національного виробництва і доходу

– показники обсягів та темпів промислового виробництва;

– галузева структура господарства та динаміка окремих галузей, капіталовкладення та ін.;

– показники якості життя: ВВП на душу населення, рівень диференціації доходів, забезпеченість основних груп населення матеріальними благами і послугами, працездатність населення, стан навколишнього середовища і т.д.

Показано, що вище зазначені показники характеризують:

– природно-ресурсний, виробничий, науково-технічний потенціал країни;

– динамічність та адаптивність господарського механізму, а також його залежність від зовнішніх факторів: рівень інфляції, дефіцит консолідованого бюджету, дію зовнішньоекономічних чинників, стабільність національної валюти, внутрішню і зовнішню заборгованість.

Визначено, що економічна безпека – це здатність економіки забезпечувати ефективне задоволення суспільних потреб на національному і міжнародному рівнях, тобто, економічна безпека являє собою сукупність внутрішніх і зовнішніх умов, що сприяють ефективному динамічному зростанню національної економіки, її здатності задовольняти потреби суспільства, держави, індивіда, забезпечувати конкурентноздатність на зовнішніх і внутрішніх ринках, що гарантує від різного роду загроз і втрат.

Науковою новизною дослідження є встановлення того факту, що економічна безпека для підприємств та організацій сфери економіки, бізнесу та фінансів повинна забезпечуватися, насамперед, ефективністю самої економіки країни, тобто, поряд із захисними заходами, здійснюваними державою, вона повинна захищати сама себе на основі високої продуктивності праці, якості продукції і т.д. Т.ч., забезпечення економічної безпеки не є прерогати-

вою якого-небудь одного державного відомства, служби і, відповідно, вона повинна підтримуватися всією системою державних органів, всіма ланками і структурами економіки.

Практичним значенням отриманих результатів є те, що з'явилася можливість встановити порогові рівні зниження безпеки та охарактеризувати їх системою показників загальногосподарського і соціально-економічного значення, які, зокрема, відображають:

– гранично допустимий рівень зниження економічної активності, обсягів виробництва, інвестування та фінансування, за межами якого неможливо самостійне економічний розвиток підприємств та організацій сфери економіки, бізнесу та фінансів на технічно сучасному, конкурентоспроможному базисі

– підтримання оборонного, науково-технічного, інноваційного, інвестиційного та освітнього потенціалу.

Отримані результати, у відповідності до вище зазначених наукової новизни та практичного значення, відповідають рівню аналогічних розробок, отриманих науковими працівниками та вченими світового рівня. Їх достовірність, точність та коректність підтверджені достатньою кількість наукових публікацій у виданнях за переліками ВАК України та у виданнях, що входять до міжнародних науковометричних баз даних.

РОЗДІЛ 3

КОНФІДЕНЦІЙНІСТЬ ТА ЗАХИСТ ДАНИХ

3.1. Елементи практичної реалізації частотного тесту генераторів криптографічних перетворень

Побудова криптостійких систем у для галузі економіки, бізнесу та фінансів може бути здійснена шляхом багатократного застосування простих криптографічних перетворень (примітивів). У якості таких примітивів Клод Шеннон запропонував використовувати підстановки (*substitution*) і перестановки (*permutation*). Часто використовуваними криптографічними примітивами є перетворення типу *циклічне зрушення* або *гамування*, тобто метод шифрування, заснований на «накладенні» γ-послідовності на відкритий текст. Як γ-послідовності найчастіше використовують псевдовипадкові послідовності (ПВП), що формуються на основі поліномів.

В даний час, однією з проблем, пов'язаною з захистом даних, що передаються в інформаційно-телекомунікаційних системах галузі економіки, бізнесу та фінансів, а також з конфіденційністю інформації, є потреба в генераторах криптографічних перетворень, які відповідають високим вимогам до рівномірності розподілу вірогідності формованих ними чисел. Ці вимоги сформовані фахівцями NIST, які в 1999 р. в рамках проекту AES (*Advanced Encryption Standard*) розробили набір статистичних тестів NIST STS (*NIST Statistical Test Suite*) для випробувань ПВП [68].

Також зазначимо, що генератори криптографічних перетворень знаходять застосування в криптографічних протоколах галузі економіки, бізнесу та фінансів для формування ключів, при хешуванні паролів, а також в алгоритмах, закладених в основу потокових симетричних криптографічних систем, вживаних для захисту конфіденційності передаваної інформації. Побудова таких генераторів – абсолютно нетривіальне завдання і його рішення вимагає копіткої праці математиків та аналітиків. Генератор, слабкий з кри-

птографічної точки зору, може значно ослабити захищеність інформаційної системи і, з цієї причини, для розробників криптографічних систем важливо мати в наявності засіб перевірки їх надійності.

Аналіз наукової і технічної літератури показав, що за останні десятиліття було розроблена і досліджена велика кількість «елементарних» генераторів криптографічних перетворень до яких відносять лінійні конгруентні генератори [71, 72], генератори Фібоначчі з запізнюванням [71], генератори, побудовані на лінійних регістрах зі зворотним зв'язком [72…75] і деякі їх різновиди. Багаторічні дослідження вчених привели до висновку про те, що всі вони не є криптографічно стійкими і можуть входити до складу формувачів криптографічних перетворень тільки як складові елементи.

Як показано в [72], ідея побудови складеного генератора базується на тому факті, що комбінація двух і більше вихідних послідовностей від генераторів різного типу за допомогою таких операцій як «+», «–», «×», «⊕», дозволяє розробити структуру генератора з «кращими властивостями випадковості». Найбільш вдалі складені генератори (з погляду криптографії) детально розглянуті в роботі Б. Шнаєра [76].

З часом в алгоритмах, що здавалися раніше надійними, знаходять нові «слабкі місця». З цієї причини в процесі розробки криптографічних протоколів стає питання про пошук нових інженерних рішень з метою побудови нових, ефективних з точки зору криптографії стійких генераторів, вільних від виявлених недоліків.

Найбільш вдалим на сьогоднішній день формувачем криптографічних перетворень є алгоритм, реалізований в потоковому шифрі RC4 [76]. Однак, все частіше з'являються повідомлення про те, що і в ньому вже знайдені уразливості. Стверджується, що вдалося встановити статистичну залежність характеру ПВП, що генерувалася в потоковому шифрі RC4, від перших символів ключа.

На відміну від інших інженерних завдань, розробка нового алгоритму формування відрізняється тим, що достовірна відповідь на питання про ефек-

тивність знайденого рішення задачі може з'явитися тільки через деякий час, коли для нього буде розроблений індивідуальний метод криптоаналізу. Розробникові залишається задовольнятися тільки результатами попереднього тестування. Про це прямо сказано в керівництві до пакету тестів, розроблених NIST [68]. Будь-який із запропонованих тестів або навіть цілий пакет тестів не замінює криптоаналізу. При цьому попереднє тестування є обов'язковим. Генератор, що не задовольняє умовам тестування непридатний. Кожен з вхідних в пакет тестів орієнтується на пошук певного виду аномалій в потоці формованих символів.

До тестових пакетів, які найбільш рекомендуються до використання, відноситься вже згадуваний пакет NIST STS. Він включає набір з 16-ти тестів і методику їх використання. Успішний результат випробувань проектованого генератора із застосуванням всього набору цих тестів дає підстави сподіватися на те, що формована генератором послідовність невідмітна від «справжньої» випадкової послідовності.

Відомі й інші пакети тестів, створені для потреб криптографії. До них відноситься набір статистичних тестів під назвою Diehard [69], призначений для визначення якості послідовності випадкових чисел. Ці тести були розроблені Дж. Марсальей (George Marsaglia). Він включає 12 тестів і доступний в Інтернеті за адресою: http://stat.fsu.edu/ pub/diehard/.

За адресою http://www.isi.qut.edu.au/resources/cryptx/ можна зв'язатися з розробниками пакету тестів CRYPT-X [70] і отримати програмне забезпечення та керівництво по їх застосуванню.

Проте використання відмічених пакетів прикладних програм натрапляє на ряд серйозних перешкод. Перша з них полягає в тому, що вони призначені для оцінки вже готових генераторів. У практичній роботі галузі економіки, бізнесу та фінансів такі пристрої розробники конструюють поетапно, поступово доводячи їх до рівня відповідності вимогам, що пред'являються.

Друга проблема полягає в тому, що в основі кожного з вхідних в пропонований пакет тестів лежить достатньо складне теоретичне обґрунтування,

що вимагає від розробників серйозної математичної підготовки та знань різних несуміжних розділів математики. На жаль, в керівництві, що додається до тестів, розробники такого обґрунтування, як правило, не приводять.

Нарешті, третя проблема, полягає в тому, що, хоча до програмного забезпечення і наданий вільний безкоштовний доступ, скористатися ним складно. Більшість тестів припускають попереднє створення файлу, в який записується випробовувана псевдовипадкова послідовність у вигляді 32-бітових слів, а потім запускається процедура тестування. Це не завжди зручно і підходить не для всіх тестів, оскільки вимагає значних програмно-апаратних ресурсів. До того ж, пропоновані тести розраховані на певну програмно-апаратну платформу.

Перераховані проблеми вимушують розробників якщо не розробляти власні тести, то, принаймні, створювати власне програмне забезпечення, яке їх реалізує, є зручним в роботі та може ефективно використовуватися в процесі пошуку конструктивного вирішення генератора, що розробляється.

Всякий пакет тестів має свою внутрішню логіку. Передбачається, що випробування нового генератора повинне починатися з частотного тестування. Як вказується в [68], якщо генератор не проходить частотний тест, то проведення всіх інших тестів вже не має сенсу. Тому, враховуючи все вищесказане, метою підрозділу є аналіз виконання частотного тестування і методики її проведення.

Тестування генератора, зокрема частотне, засноване на порівнянні цього генератора з ідеалом. Передбачається, що такий ідеальний генератор формує криптографічну послідовність з рівномірним розподілом вірогідності одиниць і нулів, причому таку, що наступний вихідний біт неможливо передбачити за наслідками спостереження деякого відрізка цієї послідовності з вірогідністю, що відрізняється від 0,5.

Насправді, реальний генератор криптографічних перетворень видає «несправжню» випадкову послідовність, а повністю визначувану значенням секретного ключа. Ступінь його схожості з реальним формувачем випадкової гами може бути встановлена на підставі вибраного еталону та критерію, який

дозволяє визначити ступінь відмінності отриманого результату від очікуваного рівномірного розподілу вірогідності.

Формальне визначення критерію припускає завдання нульової гіпотези H_0, відповідно до якої тестована послідовність є випадковою. З нею безпосередньо пов'язана альтернативна гіпотеза H_A відповідно до якої ця послідовність не може бути визнана випадковою. Приймаючи нульову гіпотезу, експериментатор з вірогідністю α, ризикує помилитися – зробити так звану «помилку першого роду». Відповідно, з вірогідністю $1-\alpha$, він буде правим. Зазвичай, величину α вибирають в межах $0,01 < \alpha < 0,001$.

При частотному тестуванні передбачається, що поява символів на виході генератора повністю підкоряється розподілу Бернуллі. При якому вірогідність одиничного символу p рівна вірогідності появи нульового символу – $q = 1 - p$. В цьому випадку різниця між числом одиниць n_1 і числом нулів n_0, $S_n = n_1 - p$ в n-розрядній послідовності складає $\varepsilon = \varepsilon_1, \varepsilon_2, ..., \varepsilon_n$, де ε_i – двійковий символ, що приймає значення $\{0,1\}$. Різниця буде підпорядкована біноміальному закону розподілу вірогідності, який відповідно до теореми Муавра-Лапласа, при достатньо великому значенні n, добре апроксимірується стандартним нормальним законом $N_{0,1}$ з нульовим математичним очікуванням і одиничною дисперсією. Як показано в [68, 77], ця різниця, відповідно до центральної граничної теореми, задовольняє умові:

$$\lim_{n\to\infty} P\left(\frac{S_n}{\sqrt{n}} < z\right) = \Phi(z) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} e^{-\frac{u^2}{2}} du,$$

де $\Phi(z)$ – функція Лапласа, яка є чисельно рівною площі фігури, обмеженої зверху кривою Гауса, знизу віссю абсцис, а справа – прямою $y = z$.

У [68] показано, що для позитивних значень z, буде справедливий вираз:

$$P\left(\frac{S_n}{\sqrt{n}} \le z\right) = 2\Phi(z) - 1.$$

За даними випробування n-розрядної двійкової послідовності необхідно обчислити статистику:

$$s_{obs} = \frac{|n_1 - n_0|}{\sqrt{n}} = \frac{|S_n|}{\sqrt{n}}.$$

Значення статистики дозволяє розрахувати вірогідність того, що параметр z не вийде за межі допустимого значення α, визначуваного вибраним критерієм. Ця вірогідність може бути представлена у вигляді:

$$2\left[1-\Phi\left(\frac{|s_{obs}|}{\sqrt{n}}\right)\right] = erfc\left(\frac{|s_{obs}|}{\sqrt{n}}\right). \qquad (3.1)$$

Враховуючи, що додаткова функція помилки визначається як

$$erfc(z) = \frac{2}{\sqrt{\pi}}\int_z^{\infty} e^{-u^2} du, \qquad (3.2)$$

то, з урахуванням меж інтеграції, вираз (3.1) можна переписати у вигляді:

$$2\left[1-\Phi\left(\frac{|S_{obs}|}{\sqrt{2n}}\right)\right] = erfc\left(\frac{|S_{obs}|}{\sqrt{2n}}\right).$$

Якщо, в результаті випробувань обчислена величина $P = erfc\left(\frac{|S_{obs}|}{\sqrt{2n}}\right) \geq \alpha$, то тестована послідовність визнається випадковою.

Якщо величина α вибрана рівною 0,01, то це означає, що зі ста тестованих послідовностей не більше ніж одна з них може бути забракована як «невипадкова».

Програмна реалізація такого тесту має дві складності. Перша з них полягає в тому, що достатньо складно реалізувати ефективний підрахунок числа одиничних n_1 і, відповідно, нульових n_0 символів в тестованій послідовності. Це пояснюється тим, що в більшості сучасних обчислювальних архітектур команд для роботи з окремими бітами немає.

Друга складність полягає в необхідності обчислення в кожному тесті значення додаткової функції помилки $erfc$. В принципі, її значення можна обчислити і за допомогою прикладного програмного пакету MatLab, але в

процесі тестування великого числа послідовностей звертатися до окремого програмного пакету не зручно.

Оскільки розмір тестованої послідовності n невеликий (у [68] рекомендується вибирати n не більше, ніж 100 символів), їх кількість в кожному байті може бути підрахована так, як це описано далі.

Зважаючи, що при двійковому численні вага кожного двійкового розряду машинного слова більше суми вагів всіх розрядів, які стоять зліва від нього (молодших по відношенню до цього розряду), значення двійкових символів, що входять до складу цього слова і їх кількість визначається по наступній методиці.

Вважатимемо, що символи a_i , k-розрядного слова $a=\{a_k,a_{k-1},...,a_1\}$, що виражає число b, пронумеровані справа наліво (від молодшого розряду до старшого). Тоді значення кожного з них можна розрахувати за правилом:

$$a_i=\begin{cases}1, & \text{при } b-2^{k-1}\geq 0,\\ 0, & \text{при } b-2^{k-1}<0.\end{cases}$$

Обчислення цієї процедури безпосередньо недоцільно, оскільки піднесення до ступеня – операція, трудомістка для обчислювальної системи. Якщо, наприклад, прочитування тестованої послідовності здійснюється побайтно, процедура підрахунку кількості одиничних n_1 і нульових n_0 бітів, написана на мові Delphi, може мати наступний вигляд:

```
b:=a-128;
if b>=0    then Begin
    a:=a-128; n1:=n1+1 End
   else n0:=n0+1;
b:=a-64;
if b>=0    then Begin
    a:=a-64; n1:=n1+1 End
   else n0:=n0+1;
b:=a-32;
if b>=0    then Begin
    a:=a-32; n1:=n1+1 End
```

```
   else n0:=n0+1;
b:=a-16;
if b>=0    then  Begin
    a:=a-16; n1:=n1+1 End
   else n0:=n0+1;
b:=a-8;
if b>=0    then Begin
    a:=a-8; n1:=n1+1 End
   else n0:=n0+1;
b:=a-4;
if b>=0    then Begin
    a:=a-4; n1:=n1+1 End
   else n0:=n0+1;
b:=a-2;
if b>=0    then Begin
    a:=a-2; n1:=n1+1 End
   else n0:=n0+1;
b:=a-1;
if b>=0    then Begin
    a:=a-1; n1:=n1+1 End
   else n0:=n0+1;
```

Тут лічильники **n1** і **n0** обнуляються на початку тестування і потім накопичують інформацію про кількість відповідних символів до закінчення тестування всієї послідовності. Така процедура виглядає декілька громіздко, проте працює швидко. Вона легко може бути розширена і на випадок блоку більшого розміру.

Алгоритм розглянутої процедури приведено на рис. 3.1.

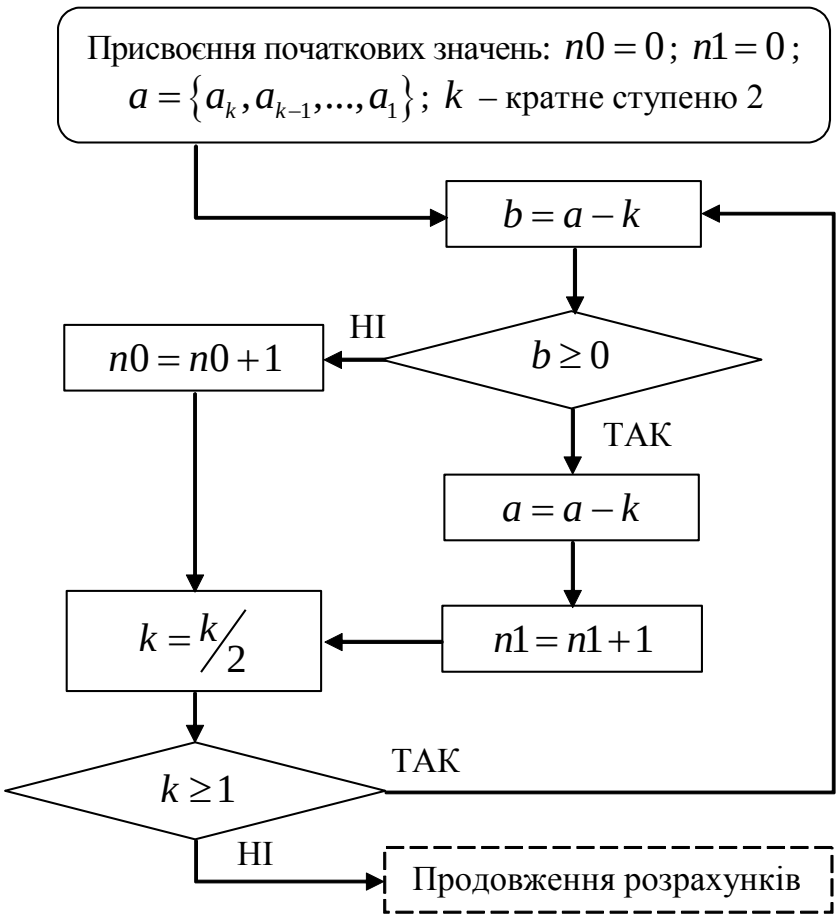


Рис. 3.1 – Алгоритм підрахунку кількості одиничних і нульових бітів

Що стосується обчислення показника P, що є додатковою функцією помилки $erfc(x)$ вигляду (3.2), то її можна представити так:

$$erfc\ (x) = 1 - erf\,(x) = \frac{2}{\sqrt{\pi}} \int_x^{\infty} e^{-t^2} dt\,.$$

Брати такий інтеграл у вказаних межах незручно, тому краще обчислити функцію $erf\,(x) = \ = \frac{2}{\sqrt{\pi}} \int_0^{x} e^{-t^2} dt$, а потім перейти до функції $erfc(x)$.

Функція $erf\,(x)$ не може бути представлена через елементарні функції. Проте її можна представити у вигляді ряду:

$$erf\,(x) = \frac{2}{\sqrt{\pi}} \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n+1}}{n!(2n+1)} = \frac{2}{\sqrt{\pi}} \left(x - \frac{x^3}{3} + \frac{x^5}{10} - \frac{x^7}{42} + \frac{x^9}{216} - ... \right).$$

Цим розкладанням можна користуватися, якщо значення аргументу функції $erf\left(x\right)$ не перевищує значення $x=3$. При більшому значенні аргументу можна скористатися асимптотичним розкладанням вигляду

$$erfc(x)=\frac{e^{-x^2}}{x\sqrt{\pi}}\left[1+\sum_{n=1}^{\infty}(-1)^n\frac{1\times3\times5\times\ldots\times(2n-1)}{(2x^2)^n}\right]=\frac{e^{-x^2}}{x\sqrt{\pi}}\sum_{n=0}^{\infty}(-1)^n\frac{(2n)!}{n!(2x)^{2n}}$$

і обчислити значення функції $erfc\left(x\right)$ безпосередньо. Якщо ряд для визначення значення функції $erf\left(x\right)$ вимагає обчислення до 30-ти членів, то останній ряд, для обчислення функції $erfc\left(x\right)$, дає хороше наближення вже при обчисленні чотирьох членів.

Представлені розкладання для функцій $erf\left(x\right)$ і $erfc\left(x\right)$ можна знайти за адресою http:// functions.wolfram.com/GammaBetaErf/.

Т.ч., як слідує з викладеного, для тестування послідовності, що формується проектованим генератором, необхідний програмний продукт, в який цей генератор входитиме як складова частина, і який дозволить формувати m n-розрядних послідовностей. Тут m – задане число тестів. При чому цей продукт повинен мати окремий вбудований генератор ключів, з тим, щоб забезпечити їх незалежність. У цьому ж продукті можна розмістити і програму для тестування, яка, з використанням викладених прийомів, дозволить визначати частку послідовностей, що не пройшли тест.

На закінчення відзначимо, що саме такий підхід поетапного тестування і підбору складових елементів генератора дозволяє зробити попередні висновки про прийнятність передбачуваної архітектури проектованого генератора або шифру. На практиці реалізований описуваний підхід до тестування у вигляді двох окремих складових – модуля генератора і модуля тесту. Це дозволяє застосовувати модуль тестування для інших типів генераторів тієї ж розрядності.

3.2. Надійність програмного забезпечення інформаційних систем галузі економіки, бізнесу та фінансів

Життєвий цикл програмного забезпечення (продукта) будь-якої галузі народного господарства, включаючи економіку, бізнес та фінанси, починається з визначення технічного завдання щодо його розробки і закінчується припиненням його використання.

Дії, які виконуються протягом життєвого циклу програмного продукту є наступними:

– п’ять основних процесів;

– вісім процесів з підтримки;

– чотири організаційні процеси.

До складу основних процесів життєвого циклу входять п’ять процесів, що обслуговують основних учасників протягом життєвого циклу програмного забезпечення. Основні учасники – це суб’єкти, які ініціюють, розробляють, проводять експлуатацію чи супровід програмного продукту. До основних учасників належать замовник, постачальник, розробник, оператор та супроводжувач програмного продукту. До основних процесів належать такі процеси:

– *замовлення* – визначає дії замовника-організації, що замовляє систему, програмний продукт або програмну послугу;

– *постачання* – визначає дії постачальника-організації, що надає систему, програмний продукт або програмну послугу;

– *розроблення* – визначає дії розробника-організації, що визначає та проектує програмний продукт;

– *експлуатації* – визначає дії оператора-організації, що надає послугу з експлуатації інформаційної (автоматизованої) системи в її існуючому середовищі для її користувачів;

– *супроводу* – визначає дії супроводжувача-організації, що надає послугу з супроводу програмного продукту, тобто, керує внесенням змін до програм-

ного продукту для підтримання його в належному та працездатному стані. Цей процес передбачає перенесення та вилучення програмного продукту.

Процес підтримки застосовується та виконується в рамках процесу відповідно до його потреб. До складу процесів підтримки життєвого циклу програмного продукту входять процеси:

– *документування* – визначає дії щодо реєстрації інформації, отриманої в процесі життєвого циклу;

– *конфігурування* – визначає дії щодо керування конфігурацією програмного продукту;

– *забезпечення якості* – визначає дії щодо набуття об'єктивної впевненості в тому, що програмні продукти та процеси відповідають заданим для них вимогам та дотримуються встановлених для них планів.

Як методи забезпечення якості можна використовувати процеси спільного перегляду, аудиту, верифікації та валідації;

– *верифікації* – визначає дії замовника, постачальника або незалежного учасника щодо проведення верифікації програмного продукту з різним ступенем глибини залежно від програмного продукту;

– *валідації* – визначає дії замовника, постачальника або незалежного учасника щодо проведення валідації програмного продукту, одержаного в рамках програмного проекту;

– *спільного перегляду* – визначає дії щодо проведення оцінки стану та результатів певної дії. Цей процес може бути застосований будь-якими двома учасниками, один з яких (учасник, що здійснює перегляд) здійснює перегляд дій іншого учасника (учасника, дії якого переглядаються) в рамках спільного обговорення;

– *аудиту* – визначає дії щодо визначення відповідності вимогам, планам та контракту. Цей процес може бути застосований будь-якими двома учасниками, один з яких (учасник, що перевіряє) проводить аудит програмного продукту або дій іншого учасника (учасник, якого перевіряють);

– *вирішення проблем* – визначає дії щодо аналізу і зняття проблем (включно з невідповідностями) незалежно від їхньої природи та причин, ви-

явлених в процесі розроблення, експлуатації, супроводу чи під час виконання інших процесів.

Організаційні процеси життєвого циклу програмного продукту застосовуються організацією для встановлення і реалізації базової структури, до склад якої входять взаємопов'язані процеси життєвого циклу та відповідний персонал, а також для постійного вдосконалення структури та процесів. Їх застосування, як правило, виходить за рамки вдосконалення конкретних проектів і контрактів; проте досвід щодо проектів та контрактів використовується для вдосконалення і ефективності роботи організації. До організаційних процесів входять процеси:

– *керування* – визначає основні дії щодо керування, включно з керуванням проектом, протягом життєвого циклу;

– *створення інфраструктури* – визначає основні дії щодо створення основної структури процесів життєвого циклу;

– *утворення* – визначає базові дії, які організація (якою може бути замовник, постачальник, розробник, оператор, супроводжувач або керівник іншого процесу) виконує з метою створення, вимірювання, контролю та вдосконалення процесів життєвого циклу, які вона проводить;

– *навчання* – визначає дії щодо забезпечення відповідного навчання персоналу.

Програми для сучасних інформаційних систем можуть нараховувати значну кількість (сотні, тисячі, десятки та сотні тисяч) простих команд. Під час написання програм з різних причин можуть з'явитися помилки. В середовищі програмістів говорять, що немає програм без помилок, а є програми із не виявленими помилками. Грубі помилки виявляються на стадії відпрацювання програми, але перевірити програму на всіх можливих режимах, як правило, не удається, то нема впевненості, що всі помилки в ній знайдені. При цьому використовується статистичний підхід до аналізу процесу виявлення помилок в програмі. Цей процес може бути охарактеризований функцією $\frac{f(t)}{R}$, де $f(t)$ – кількість виявлених і виправлених помилок в одиницю часу

в програмі, яка має R – кількість команд $\frac{f(t)}{R}=\frac{d\varepsilon_n}{dt}= =\frac{\varepsilon_n(t+\Delta t)-\varepsilon_n(t)}{\Delta t}$, де $\varepsilon_n(t)$ – кількість виявлених і виправлених помилок за час t в розрахунку на одну команду. Відповідно, $\varepsilon_n(t)=\frac{1}{R}\int_0^t f(t)dt$.

Функція $f(t)$ може бути дослідно визначена під час відпрацювання програми шляхом фіксації кількості виявлених помилок. Задача визначення $f(t)$ спрощується, якщо $f(t)=\frac{\varepsilon_0}{\tau_0}e^{-\frac{t}{\tau_0}}$, де ε_0 і τ_0 – параметри $f(t)$, які визначаються під час відпрацювання. Тоді $\varepsilon_n(\tau)=\frac{1}{R}\int_0^\tau f(t)dt=\frac{\varepsilon_0}{R}\left(1-e^{-\frac{\tau}{\tau_0}}\right)$.

При $\tau\to\infty$ $\varepsilon_n(\infty)=\frac{\varepsilon_0}{R}$ або $\varepsilon_0=R\varepsilon_n(\infty)$. Звідки слідує, що ε_0 – це загальне число помилок в програмі перед початком відпрацювання. Так як процес відпрацювання не може бути тривалим, та в програмі завжди буде залишатися деяка кількість помилок $\varepsilon(\tau)=\frac{\varepsilon_0}{K}-\varepsilon_n=\frac{\varepsilon_0}{R}e^{-\frac{\tau}{\tau_0}}$, де $\varepsilon(t)$ – кількість знайдених помилок в розрахунку на одну команду. Якщо передбачити, що похибки рівномірно розподілені по всій програмі, то ймовірність $P(t)$ появи похибки за час Δt буде пропорційна швидкодії δ інформаційної системи (середньому числу змін в одиницю часу команд) і кількості залишених в програмі помилок, тобто $P(\tau)=\varepsilon(\tau)\delta\Delta t$.

Проводячи аналогію між процесом появи помилок і відмов об'єктів $(P(t)=\lambda\Delta t)$ можливо зробити висновок, що інтенсивність похибок $\varepsilon(t)$ не залежить від часу t і визначається тільки інтервалом Δt, на якому оцінюється імовірність появи помилки. Звідки, наробіток на «відмову», котрий обумовлений появою помилки в програмі, буде складати $T(\tau)=\frac{1}{\varepsilon(\tau)\delta}=\frac{R}{\varepsilon_0\delta}e^{\frac{\tau}{\tau_0}}$.

Аналіз зміни $T(\tau)$ може служити основою для вибору часу τ відпрацювання програми, а саме, відпрацювання закінчується, якщо величина $T(\tau)$ становиться достатньо великою.

У випадку, коли вдається оцінити матеріальні втрати C_n від появи помилки в розрахунках, то час τ відпрацювання можливо оцінити кількісно наступним чином. За час T_p роботи програми вона відмовить $\frac{T_p}{T(\tau)}$ разів, що викличе сумарну втрату $C_n \frac{T_p}{T(\tau)}$. Процес відпрацювання програми вимагає затрат часу обчислень та інших затрат пов'язаних з ним. Якщо вартість одного часу відпрацювання позначити C_0, то за час τ таких затрат буде $C_0\tau$. Відповідно, загальна втрата C від помилки і затрат на відпрацювання програми будуть становити $C = \frac{CT_p}{T(\tau)} + C_0\tau = \frac{C_n T_p \varepsilon_0 \delta}{R} e^{-\frac{\tau}{\tau_0}} + C_0\tau$.

Звідки вище приведеного виразу слідує, що $\frac{dC}{d\tau} = \frac{-C_n N_p \varepsilon_0 \delta}{R\tau_0} e^{-\frac{\tau_M}{\tau_0}} + C_0 = 0$ або $\tau_M = -\tau_0 \ln \frac{C_0 R \tau_0}{C_n T_p \varepsilon_0 \delta}$, де τ_M – час відпрацювання, котра забезпечить мінімум C.

У цьому випадку, коли необхідно виключити помилку в програмі бажано використовувати «резервування». Одна задача вирішується декількома програмами, кожна з який розробляється незалежними групами програмістів та в основу котрих покладені різні алгоритми, а результати розрахунків програм порівнюються та рахуються вірними, коли вони співпадають. Так як поява помилки в програмах є подією маловірогідною, то поява двох або більше таких подій є подією практично неможливою.

3.2.1. Використання стійких до збоїв програм

Стійкі до збоїв програм одержують, як правило, шляхом багаторазового повторення обчислень на рівні мікрооперацій, операцій, команд, модулів програм або всієї програми.

Продуктивність інформаційної системи при використанні методу подвійного виконання залежить від числа модулів, на які розбивається програма. Дійсно, велика довжина модулів обумовлює і досить велику ймовірність появи збою. Отже, замість двох необхідно буде три і більше рази повторювати обчислення, через що час вирішення задачі буде збільшуватися. З іншого боку, при малій довжині модулів значна частина часу буде йти на порівняння і запис у пристрої пам'яті результатів обчислень, виконаних на окремих модулях програми.

У зв'язку з цим виникає задача знаходження оптимального числа модулів, на яке варто розбивати програму і при якому час T_p вирішення задачі буде мінімальним. Введемо позначення: T – час вирішення задачі за однократне виконання програми; t – тривалість обчислень на одному модулі; $p(t)$ – ймовірність відсутності збою за час t. Тоді відношення $\frac{T}{t}$ буде визначати число модулів, на яке розбивається програма. Визначимо ймовірності дво-, три-, або навіть, i-кратного повторення виконання якого-небудь модуля програми. Якщо збої – незалежні події, то ймовірність того, що даний модуль програми буде виконуватись двічі, дорівнює ймовірності відсутності збою при першому і другому виконаннях, тобто $p_2(t) = p_1^2(t)$. У подальшому ймовірність $p_1(t)$ при фіксованому t буде позначатись як p_1.

Аналогічно, g дорівнює ймовірності того, що в одному із двох попередніх обчислень відбувся збій, а в третьому обчисленні отримано правильний результат, тобто $p_3 = 2p_1^2(1-p_1) = 2p_1^2 q$, де $q = 1-p$. В загальному випадку p_3 дорівнює ймовірності того, що в i-му і одному з попередніх обчисленнях

збої були відсутні, а в інших минулих збої були, тобто $p_3 = (i-1)\,p_1^2 q^{i-2}$. Отже, середнє число обчислень буде дорівнювати $A = \sum_{i=2}^{\infty} p_i = \sum_{i=2}^{\infty} i(i-1) p_1^2 q^{i-2}$.

Легко показати, що $\frac{A}{p_1^2} = \frac{2}{(1-q)^3}$. Звідси маємо $A = \frac{2}{p_1}$. Т.ч., витрати часу на обчислення складатимуть $\frac{2T}{p_1}$. Час T_3, необхідний для виконання операцій порівняння і запису проміжних обчислень у запам'ятовуючому пристрої, залежить від типу запам'ятовуючому пристрої, що використовується, кількості k проміжних результатів і числа кроків $\frac{T}{t}$ програми, тобто $T_3 = \frac{T}{t} f\left(k, \frac{T}{t}\right)$, де $f\left(k, \frac{T}{t}\right)$ – середній час виконання операцій порівняння і звернення до пристрою пам'яті для запису результатів одного модуля програми. Якщо вважати, що $f\left(k, \frac{T}{t}\right) = const = a$, то $T_p = \frac{2T}{p_1(t)} + \frac{T_a}{t} = T\left(\frac{2}{p_1 t} + \frac{a}{t}\right)$.

Для деяких типів інформаційних систем експериментально встановлено, що $p(t) = e^{-\lambda \cdot t}$, де λ – інтенсивність збоїв. В цьому випадку T_p приймає мінімальне значення для t, яке можна визначати з рівняння $\frac{dT_p}{dt} = 2\lambda e^{\lambda \cdot t} - \frac{a}{t^2} = 0$.

Отже значення T_p, можна визначити оптимальну довжину дільниці програми і відповідне їй число $\frac{T}{t}$ дільниць, при якому T_p буде мінімальним.

Причиною невірного функціонування інформаційної системи може бути наявність в ній так званих вірусних програм, програм призначених для надмірного викривлення результатів розрахунків, видалення файлів, створення умов для ненормального функціонування інформаційної системи.

У відповідності з кодифікатором злочинів інформаційних систем Генерального секретаріату Інтерполу, віруси відносяться до категорії QD – зміна

даних інформаційних систем, всередині якої вони класифікуються наступним чином:

– QDL – логічна бомба;

– QDT – троянський кінь;

– QDV – вірус інформаційної системи;

– QDW – черв'як інформаційної системи;

– QDZ – інші види зміни даних.

Логічна бомба – здійснює тайне вставлення в програму набору команд, яке повинно спрацювати лише одного разу, але при визначених умовах.

Троянський кінь – здійснює введення до чужої програми таких команд, які дозволяють здійснити інші, не плановані власником програми функції, але одночасно зберегти і попередню працездатність.

Вірус інформаційної системи – це спеціально написана програма, котра може «приписувати» себе до інших програм (тобто «заражати» їх), розмножуватися і народжувати нові віруси для виконання різних небажаних дій в інформаційній системі.

Черв'як інформаційної системи – представляє собою спеціальну самостійно розповсюджуючи програму, що здійснює зміни даних або програм інформаційної системи, без права на це, шляхом передачі, впровадження або розповсюдження за допомогою мережі інформаційних систем.

Доля помилок або зависань інформаційної системи за рахунок вірусів складає приблизно від 10 до 30%. Відомо більш 10000 вірусів і близько 100 антивірусних програм, призначених для боротьби з ними. Існують віруси (самопошифруювані, поліморфні віруси, макровіруси тощо), здатні протидіяти противірусним програмам. Один із різновидів таких вірусів – «поселення» в противірусній програмі. Зазвичай антивірусна програма видає сигнал про своє власне зараження, якщо таке зараження здійснюється. Час необхідний для вилікування від вірусу складає в середньому від 15 до 30 хв. Самий небезпечним вірусом є вірус, який знаходиться у виконавчому файлі. В основному віруси «працюють» коректно і не викликають зависань інформаційної си-

стеми. Але серед них попадаються такі, що повністю стирають системні області жорсткого диску або підкаталоги інформаційних масивів. У 90% випадків віруси впроваджуються в інформаційні системи через мережі. Причому локальні мережі самі по собі не є розповсюджувачами вірусів. Але користувачі, що працюють із магнітними носіями, які вражені вірусом, доставляють багато клопоту такій мережі.

Ознакою зараження інформаційної системи вірусом є:

– зростання помилок і зависання інформаційної системи;

– сповільнення загрузки програми;

– неполадки (різні сповільнення і похибки) при роботи принтера;

– мигання лампочки дисковода, коли не повинні проходити операції читання/запису;

– зміна розмірів програм, що виконуються, зменшення основної доступної пам’яті.

Самими короткими є руйнуючі віруси. Їх довжина не перевищує 20 кілобайт. Самі довгі віруси досягають 100 кілобайт і більше. В останній час багато клопоту доставляють користувачам макровіруси.

Якість противірусної програми визначається по наступним характеристикам, наведеним у порядку зменшення їх важливості:

– надійність і зручність роботи (відсутність технічних проблем, вимагаючи від користувача спеціальної підготовки);

– кількість знайдених вірусів всіх типів, можливість перевірки файлів документів/таблиць, упакованих файлів, також можливість лікування заражених об’єктів;

– швидкість роботи і різні корисні функції.

Коли користувач має декілька ефективних противірусних програм і користується ними, самим надійним захистом від вірусів є профілактика зараження:

– регулярне створення резервних копій (наприклад, один раз в неділю – повне, кожен день – часткове копіювання). Наявність незаражених копій до-

зволить просто переписати «хворий» файл, наявність заражених, але не порчених копій дозволить відновити файли після видалення вірусу;

– створення резервних копій інсталяційних магнітних носіїв інформації перед установкою нового програмного забезпечення (при встановлені програми на заражену інформаційну систему вихідний магнітний носій інформації може заразитися під час інсталяції);

– перевірка по E-mail файлів, які пересилаються, на наявність вірусів;

– застосування захищених від запису магнітних носіїв інформації під час копіювання файлів на жорсткий диск. Це попередить проникнення вірусу на магнітний носій і послідуюче зараження інших інформаційних систем;

– перевірка магнітних носіїв перед загрузкою з них файлів;

– постійне використання резидентної частини противірусної програми, котра слідкує за всім підозрілим при роботі інформаційної системи.

3.2.2. Оцінка надійності програмного забезпечення за результатами налагодження та нормальної експлуатації

У процесі налагодження та дослідної або нормальної експлуатації програмного забезпечення з’являється можливість використати статистичні дані про виявлені та виправлені помилки і уточнити проектні оцінки надійності. З цією метою розроблені моделі надійності, що містять параметри, точкові оцінки яких отримують шляхом обробки результатів налагодження та експлуатації програмного забезпечення. Моделі відрізняються одна від одної припущеннями про характер залежності інтенсивності появи помилок від тривалості налагодження та експлуатації. Деякі моделі містять певні вимоги до внутрішньої структури програмних модулів.

3.2.3. Експоненціальна модель Шумана

Дана модель базується на наступних припущеннях:

– загальне число команд у програмі на машинній мові постійне;

– на початку випробувань число помилок дорівнює деякій постійній величині та по мірі виправлення помилок стає меншим; у ході виправлення програми нові помилки не вносяться;

– інтенсивність відмов програми пропорційна числу залишкових помилок.

Про структуру програмного модуля зроблені наступні припущення:

– модуль містить тільки один оператор циклу, в якому є оператори вводу інформації, оператори присвоєння та оператори умовної передачі управління вперед;

– відсутні вкладені цикли, але може бути k паралельних шляхів, якщо маємо $k-1$ оператор умовної передачі управління.

При виконанні зазначених припущень ймовірність безвідмовної роботи знаходять за формулою

$$R(t,\tau)=\exp(-C\varepsilon_r(\tau)t)=e^{-t/T};\ \varepsilon_r(\tau)=\frac{E_0}{I}-\varepsilon_B(\tau);\ T=\frac{1}{\left(C\left(\frac{E_0}{I}-\varepsilon_B(\tau)\right)\right)}, \tag{3.3}$$

де E_0 – число помилок на початку налагодження; I – число машинних команд у модулі; $\varepsilon_B(\tau)$, $\varepsilon_r(\tau)$ – число виправлених і залишених помилок у розрахунку на одну команду; T – середній наробіток на відмову; τ – час налагодження; C – коефіцієнт пропорційності.

Для оцінки E_0 і C використовують результати налагодження. Нехай із загального числа прогонів системних тестових програм r – число успішних прогонів, $n-r$ – число прогонів, що перервані помилками. Тоді загальний час n прогонів, інтенсивність помилок і наробіток на помилку знаходять за формулами

$$H=\sum_{i=1}^{r}T_i+\sum_{i=1}^{n-r}t_i;\ \lambda=\frac{n-r}{H};\ T=\frac{1}{\lambda}=\frac{H}{n-r}. \tag{3.4}$$

Припустивши, що $H=\tau_i$ і $H=\tau_2$, знайдемо:

$$\tilde{\lambda}_1=\frac{n_1-r_1}{H_1};\ \tilde{\lambda}_2=\frac{n_2-r_2}{H_2};\ \tilde{T}_1=\frac{1}{\tilde{\lambda}_1};\ \tilde{T}_2=\frac{1}{\tilde{\lambda}_2}, \tag{3.5}$$

де $\tilde{T}_1$ і $\tilde{T}_2$ – час тестування на одну помилку. Підставивши сюди (3.3) та розв'язавши систему рівнянь, отримаємо оцінки параметрів моделі:

$$\tilde{E}_0=\frac{I}{\gamma-1}\left(\gamma\varepsilon_B(\tau_1)-\varepsilon_B(\tau_2)\right);\ \tilde{C}=\frac{1}{\left(\tilde{T}_1\left(\frac{\tilde{E}_0}{I}-\varepsilon_B(\tau_1)\right)\right)};\ \gamma=\frac{\tilde{T}_1}{\tilde{T}_2}, \tag{3.6}$$

Для обчислення оцінок необхідно по результатам налагодження знати $\tilde{T}_1,\ \tilde{T}_2,\ \varepsilon_B(\tau_1)$ і $\varepsilon_B(\tau_2)$.

Деяке узагальнення результатів (3.4) – (3.6) полягає в наступному. Нехай T_1 і T_2 – час роботи системи, що відповідає часу налагодження τ_1 і τ_2, n_1 і n_1 – число помилок, виявлених у періодах τ_1 і τ_2. Тоді $\frac{T_1}{n_1}=\frac{1}{\left(C\left(\frac{E_0}{I}-\varepsilon_B(\tau_1)\right)\right)}$, $\frac{T_2}{n_2}=\frac{1}{\left(C\left(\frac{E_0}{I}-\varepsilon_B(\tau_2)\right)\right)}$. Звідси:

$$\tilde{E}_0=\frac{I}{\gamma-1}\left(\gamma\varepsilon_B(\tau_1)-\varepsilon_B(\tau_2)\right);\ \tilde{C}=\frac{\frac{n_1}{T_1}}{\left(\frac{\tilde{E}_0}{I}-\varepsilon_B(\tau_1)\right)};\ \gamma=\frac{T_1}{n_1}\Big/\frac{T_2}{n_2}. \tag{3.7}$$

Якщо T_1 і T_2 – лише сумарний час налагодження, то $\tilde{T}_1=T_1/n_1$, $\tilde{T}_2=T_2/n_2$, то формула (3.7) співпадає з (3.6).

Якщо в ході налагодження проводиться k тестів в інтервалах $(0,\tau_1)$, $(0,\tau_2),\ldots(0,\tau_k)$, де $\tau_1<\tau_2<\ldots<\tau_k$, то для визначення оцінок максимальної правдоподібності використовують рівняння

$$\tilde{C} = \sum_{j=1}^{k} n_j \Big/ \left(\frac{\tilde{E}_0}{I} - \varepsilon_B(\tau_j) \right) H_j ;\ \tilde{C} = \left\{ \sum_{j=1}^{k} n_j \Big/ \left(\frac{\tilde{E}_0}{I} - \varepsilon_B(\tau_j) \right) \right\} \sum_{j=1}^{k} H_j , \qquad (3.8)$$

де n_j – число прогонів j-го тесту, що закінчуються відмовами; H_j – час, що затрачається на виконання успішних і неуспішних прогонів j-го тесту. При $k = 2$ (3.8) зводиться до попереднього випадку і розв'язок дає результат (3.7).

Асимптотичне значення дисперсій оцінок (для великих значень n_j) визначаються виразами

$$D\tilde{C} = 1 \Big/ \left\{ \sum_{j=1}^{k} n_j \Big/ C^2 - \left(\sum_{j=1}^{k} H_j \right)^2 \Big/ \sum_{j=1}^{k} \left(n_j \Big/ \left(\frac{E_0}{I} - \varepsilon_B(\tau_j) \right)^2 \right) \right\};$$

$$DE_0 = 1 \Big/ \sum_{j=1}^{k} \left\{ \left(n_j \Big/ \left(\frac{E_0}{I} - \varepsilon_B(\tau_j) \right)^2 \right) - C^2 \left(\sum_{j=1}^{k} H_j \right)^2 \Big/ \sum_{j=1}^{k} n_j \right\},$$

де $C \cong \tilde{C}$, $E_0 \cong \tilde{E}_0$.

Коефіцієнт кореляції оцінок

$$\rho(\tilde{C}, \tilde{E}) \cong \left\{ \sum_{j=1}^{k} n_j \Big/ \left(\frac{E_0}{I} - \varepsilon_B(\tau_j) \right) \right\} \Big/ \left\{ \sum_{j=1}^{k} n_j \sum_{j=1}^{k} \left(n_j \Big/ \left(\frac{E_0}{I} - \varepsilon_B(\tau_j) \right)^2 \right) \right\}^{0,5} .$$

Асимптотичне значення дисперсії і коефіцієнта кореляції використовуються для визначення довірчих інтервалів значень E_0 і C на основі гауссівського розподілу.

У ряді робіт зазначається, що найбільш адекватною для моделі Шумана є експоненціальна модель зміни кількості помилок при зміні тривалості налагодження $\varepsilon_B(\tau) = \frac{E_0}{I}\left(1 - e^{-\tau/\tau_0}\right)$, де E_0 і τ_0 визначаються дослідним шляхом. Тоді $R(t,\tau) = \exp\left(-CE_0 / Ie^{-I/I_0} t\right)$.

Середній наробіток на відмову зростає експоненціально зі збільшенням тривалості налагодження: $T = I \Big/ CE_0 e^{\frac{\tau}{\tau_0}}$.

3.2.4. Експоненціальна модель Джелінського-Моранди

Дана модель є частинним випадком моделі Шумана. Згідно цієї моделі, інтенсивність появи помилок пропорційна числу залишкових помилок: $\lambda(\Delta t_i) = K_{JM}(E_0 - i + 1)$, де K_{JM} – коефіцієнт пропорційності; Δt_i – інтервал між i-ю та $(i-1)$-ю виявленими помилками. Ймовірність безвідмовної роботи

$$R(t) = \exp(-\lambda(\Delta t)) = \exp(-K_{JM}(E_0 - i + 1)),\ t_{i-1} < t < t_i. \qquad (3.9)$$

При $K_{JM} = C/I$ і $\varepsilon_B(\tau) = (i-1)/I$ формула (3.9) співпадає з (3.3). Для того щоб отримати оцінки максимальної правдоподібності для параметрів E_0 і τ_0 при послідовному спостереженні k помилок у моменти $t_1, t_2, ..., t_k$, потрібно розв'язати систему рівнянь $\sum_{i=1}^{k}\left(\hat{E}_0 - i + 1\right)^{-1} = k \Big/ \left(\hat{E}_0 - i + 1\right)$; $\hat{K}_{JM} = \frac{k}{A} \Big/ \left(E_0 - \theta \cdot k + 1\right)$;

$\theta = \frac{B}{AK}$; $A = \sum_{i=1}^{k} t_i$; $B = \sum_{i=1}^{k} i t_i$.

Асимптотичні оцінки дисперсії і коефіцієнта кореляція (при великих) k визначаються за допомогою формул: $D\hat{E}_0 \cong \frac{k}{kS_2 - A^2C^2}$; $D\hat{K}_{JM} \cong \frac{S_2 K_{JM}^2}{kS_2 - A^2 K_{JM}^2}$;

$\rho\left(\hat{K}_{JM}, \hat{E}_0\right) \cong \frac{AK_{JM}}{(kS_2)^{0,5}}$; $S_2 = \sum_{i=1}^{k}(E_0 - i + 1)$.

Для того щоб отримати числові значення цих величин, необхідно скрізь замінити E_0 і K_{LM} їх оцінками.

3.2.5. Вейбулівська модель

Модель задається сукупністю співвідношень: $\lambda(t) = m\lambda^m t^{m-1}$; $R(t) = e^{-(\lambda t)_m}$; $T = \frac{1}{\lambda}\Gamma\left(1 + \frac{1}{m}\right)$. Перевага цієї моделі полягає в тому, що вона містить додатковий в порівнянні з експоненціальною моделлю параметр m. Підбираючи значення двох параметрів: m-параметр форми і λ-параметр масштабу, можна отримати більш точну відповідність експериментальним даним. Значення

m підбирають з діапазону $0 < m < 1$. Оцінки параметрів отримують за допомогою метода моментів. Для параметра форми m значення знаходять як розв'язок рівняння $\Gamma\left(1+\frac{2}{m}\right)\Big/\Gamma^2\left(1+\frac{1}{m}\right)=\frac{s^2}{\bar{t}^2}$; $\bar{t}=\frac{1}{k}\sum_{i=1}^{k}t_i$; $s^2=\frac{1}{k}\sum_{i=1}^{k}\left(t_i-\bar{t}\right)^2$, де $\Gamma(x)$ – гама-функція. Для параметра масштабу λ його оцінка визначається за формулою $\hat{\lambda}=\Gamma\left(1+\frac{1}{m}\right)\Big/\bar{t}$.

3.2.6. Структурна модель Нельсона

В якості показника надійності приймається ймовірність $R(n)$ безвідмовного виконання n прогонів програми. Для j-го прогону ймовірність відмови представляють наступним чином $Q_j=\sum_{i=1}^{N}\rho_{ji}y_i$, де y_i – індикатор відмови при i-ому наборі даних; p_{ji} – ймовірність появи i-го набора в j-ому прогоні. Тоді $R(n)=\prod_{j=1}^{n}(1-Q_j)=\exp\left(\sum_{j=1}^{n}\ln(1-Q_j)\right)$.

Якщо Δt_j – час виконання j-го прогону, то інтенсивність відмов

$$\lambda\left(t_j\right)=\frac{-\ln\left(1-Q_j\right)}{\Delta t_j};\ R(n)=\exp\left(\sum_{j=1}^{n}\lambda(t_j)\Delta t_j\right);\ t_j=\sum_{i=1}^{j}t_i. \qquad (3.10)$$

Практичне використання формули (3.10) ускладнюється через множину входів і велику кількість складно оцінюваних параметрів моделі. На практиці надійність програм оцінюється по результатам тестових випробувань, що охоплюють відносно невелику область простору початкових даних.

Для спрощеної оцінки пропонується формула $R(N)=\frac{1}{N}\sum_{i=1}^{N}E_i(n_i)W_i$; $\sum_{i=1}^{N}W_i=N$, де N – число прогонів; n_i – число виявлених помилок при i-ому прогоні; E_i – індикатор відсутності помилок при прогоні i-го тесту.

Для зменшення розмірності задачі множини значень вхідних наборів розбивають на непересічні підмножини G_j, кожній з яких відповідає визначений шлях L_j, $j=1...n$. Якщо L_j містить помилки, то при виконанні тесту на підмножині G_j буде відмова. Тоді ймовірність правильного виконання одного тесту $R(1)=1-\sum_{j=1}^{n} p_j\varepsilon_j$, $p_j=\sum_{i\in G_j} p_{ij}$, $\varepsilon_j<1$.

При такому підході знайти оцінку надійності по структурній моделі досить складно, так як помилка в L_j проявляється не при будь-якому наборі з G_j, а лише при деяких. Крім того, відсутня методика оцінки ε_j по результатам випробувань програм.

Слід відмітити, що на сьогодні для цієї моделі ще не знайдено достатньо аргументованого обґрунтування її практичної реалізації.

3.3. Теореми до теорії випробовування надійності автоматичних банківських систем однократного використання

До необхідності доказу окремих теорем, які можуть бути використані при розгляді та аналізі деяких аспектів інтервального оцінювання робочих параметрів надійного включення резервної системи при випробуваннях автоматичних банківських систем однократного використання, приводять випадки сугубо практичного характеру. Так, у зазначеному сенсі, далі будемо розглядати процедуру випробовування системи, яка автоматично виконує деяку одну функцію. Однократне максимально достовірне та надійне виконання зазначеної функції є основним та єдиним завданням системи. Після її виконання сенс в роботі системи втрачається, а сама система ліквідується. До таких систем відноситься широке коло механічних, електронних, біологічних, хімічних та інших простих та складних механізмів, приладів, сполук, включаючи математичні системи (наприклад, в системах захисту інформації – автоматичний шифроблокнот) та ін. У тому випадку, коли система не включилася, по-

винне бути задіяне резервне устаткування. Далі аналізуються аспекти надійного включення саме таких систем. При цьому розуміється, що резервне обладнання має ті ж самі властивості щодо його однократного використання. Про живучість зазначених систем в підрозділі мова не йде.

З огляду на те, що необхідність у включенні резервного устаткування такої системи є випадковою величиною, то проведення випробувань та планових перевірок апаратури повинне забирати мінімальний час. Його скорочення можливе за рахунок структурної надмірності або за рахунок запасу по ресурсу [78-81]. Вид випробувань обирається з врахуванням конкретних задач та в залежності від способу побудови системи, яка підлягає випробовуванню. Т.ч., з метою вибору найбільш ефективного виду випробувань, необхідно вирішення всіх наукових та практичних задач, які стосуються оцінки надійності резервних компонентів (функціональних об‘єктів) у загальній структурі автоматичної банківської системи і, в тому числі, з їх послідовно-паралельним з’єднанням.

Метою досліджень в цьому підрозділі є отримання результатів, які будуть доцільними:

– для визначення та обґрунтування робочих планів випробувань;

– для планування необхідної кількості резервних складових;

– для побудови та удосконалення загальної структури автоматичної банківської системи;

– для встановлення в загальному вигляді інших технічних та виробничих параметрів.

Зазначена мета одночасно є раніше невирішеною частиною загальної проблеми надійного функціонування автоматичних систем та резервуючих об‘єктів, які входять до їх складу. Передбачається, що отриманні результати можуть бути впроваджені у наукові розробки та у виробництво, що приведе до зменшення фінансових витрат при проведенні випробувань банківських систем про які йде мова.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми, показав, що про методики проведення випробувань, які по своїй суті аналогічні тим, які розглядаються в підрозділі, технічні та математичні проблеми обробки отриманих результатів є достатньо відомостей у спеціальній літературі. Слід зазначити, що всі методики передбачають припинення функціонування об'єкта в складі автоматичної системи при проведенні випробувань і *повернення його в її склад* після закінчення випробувань для подальшого використання. Така процедура випробувань лише в деякому ступені відповідає проблемі, що винесена в заголовок підрозділу, так як передбачає випробування лише одного об'єкта. Нею займалося достатньо широке коло вчених – Р.А. Мирний, І.В. Павлов, Л.Н. Большев, Р.С. Судаков та інші. Окремі результати щодо оцінки надійності окремих резервних систем телекомунікацій з послідовним з'єднанням об'єктів за результатами їх біноміальних іспитів з зупинкою опубліковані авторами самостійно або в співавторстві в [78-84]. Однак, у публікаціях, які доступні для широкого кола науковців, оцінка надійності автоматичних систем однократного використання з послідовно-паралельним з'єднанням резервуючих об'єктів раніше не розглядалася.

Постановкою завдання підрозділу є доказ окремих теорем, які можуть бути використані при розгляді та аналізі деяких аспектів інтервального оцінювання робочих параметрів при випробуваннях надійності автоматичних систем однократного використання (включаючи банківські системи) з послідовно-паралельним з'єднанням резервуючих об'єктів по схемі біноміальних іспитів з зупинкою.

Як було зазначено вище, будемо розглядати автоматичну систему з комплектом резервного обладнання, завданням якої є однократне достовірне та надійне виконання встановленої функції, після чого система ліквідується. Кожен з комплектів, включаючи основний, назвемо *об'єктами*. З метою забезпечення зазначеного вважатимемо, що система складена з m об'єктів, сполучених послідовно, вважаючи, що кожен з об'єктів, у свою чергу, містить v_j еле-

ментів, сполучених паралельно (рис. 3.2), що, як відомо, є одним зі способів підвищення надійності роботи автоматичних систем.

Позначимо A_{ij} як подію, що складається в успішному функціонуванні j-го елемента в i-му об‘єкті та $R_{ij} = P\left(A_{ij}\right)$ – як імовірність події A_{ij}. Будемо вважати, що при $i = \overline{1,m}$, $j = \overline{1,v_i}$ події A_{ij} незалежні. В цьому випадку елементи системи рис. 3.2 будемо називати *незалежними*. Спочатку зупинимося на випадку, коли вихід з ладу кожного i-го об‘єкту можливий лише в разі відмови всіх його v_i елементів.

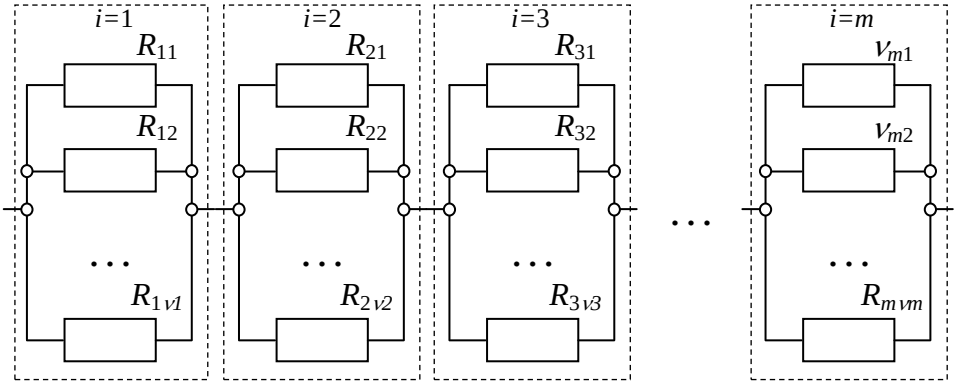


Рис. 3.2 – Загальний вигляд з’єднання об‘єктів
у резервованій банківській автоматичній ІТ-системі

Позначимо як C подію, яка полягає в успішному функціонуванні системи в цілому. Тоді при зазначених допущеннях можна вважати, що

$$C = \bigcap_{i=1}^{m} \bigcup_{j=1}^{v_i} A_{ij}\,, \tag{3.11}$$

а $\widehat{P}_0 = P(C)\prod_{i=1}^{m}\widehat{P}_i$, $\widehat{P}_i = \prod_{j=1}^{v_i}\left[1-\left(1-R_{ij}\right)\right]$, де $\widehat{P}_0$ – імовірність успішного функціонування системи в цілому ($\widehat{P}_0$ – показник надійності системи); $\widehat{P}_i$ – імовірність успішного функціонування i-го об‘єкту; $R_{ij} = P\left(A_{ij}\right)$ – імовірність ус-

пішного функціонування j-го елемента з i-го об‘єкту. Перепишемо сказане в такому вигляді:

$$\widehat{P}_0 = \prod_{i=1}^{m}\left(1-\prod_{j=1}^{v_i} q_{ij}\right),\ q_{ij} = 1-R_{ij}. \qquad (3.12)$$

Слідуючи роботі [85], покажемо, що є можливість оцінити знизу вираз (3.12) за допомогою деякої функції від добутку ймовірностей R_{ij}.

Теорема 1. Нехай v – менше з чисел v_i і з кожного об‘єкту вибрані довільні v елементів (рис. 3.3).

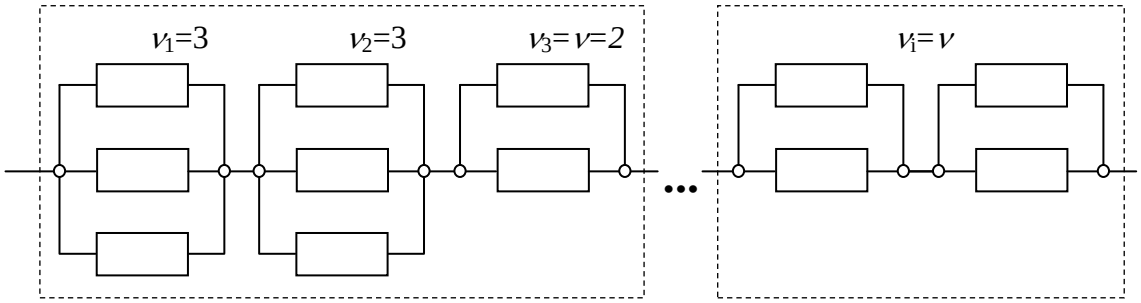


Рис. 3.3 – Процедура вибору довільних v елементів
з кожного об‘єкту системи з рис. 3.2

Якщо позначити $\Pi_0 = \prod_{i=1}^{m}\prod_{j_0=1}^{v} R_{ij0}$, $j_0 = \overline{1,v}$, то отримаємо нерівність:

$$\widehat{P}_0 = \prod_{i=1}^{m}\left(1-\prod_{j=1}^{v_i} q_{ij}\right) \geq 1-\left(\Pi_0^{1/v}\right)^{v}. \qquad (3.13)$$

Доведення. Врахуємо, що для будь-яких множин A_{ij} справедливе включення [88] вигляду $d = \bigcap_{j=1}^{v}\bigcap_{i=1}^{m} A_{ij} \subset \bigcap_{i=1}^{m}\bigcap_{j=1}^{v} A_{ij} = C_1$, звідки для подій A_{ij} витікає, що $P(D) \leq P(C_1)$ або (через незалежність цих подій):

$$P\left(\bigcap_{j=1}^{v}\bigcap_{i=1}^{m} A_{ij}\right) = 1-P\left(\bigcap_{j=1}^{v}\bigcap_{i=1}^{m} A_{ij}\right) = 1-\prod_{j=1}^{v}(1-\prod_{i=1}^{m} P\left(A_{ij}\right) \leq \prod_{i=1}^{m} P\left(\bigcap_{j=1}^{v} A_{ij}\right) = \prod_{i=1}^{m}\left(1-\prod_{j=1}^{v} P\left(A_{ij}\right)\right).$$

Зі сказаного слідує, що при $P\left(A_{ij}\right)\triangleq 1-a_{li} \rightarrow 1-\left(1-\prod_{i=1}^{m}\left(1-a_i\right)\right)^{\nu} \leq$

$\leq \prod_{i=1}^{m}(1-a_i^{\nu}$. Отже

$$\left[1-\prod_{i=1}^{m}\left(1-a_i^{\nu}\right)\right]^{1/\nu} \leq 1-\prod_{i=1}^{m}\left(1-a_i^{\nu}\right), a_i \in [0,1]. \qquad (3.14)$$

Візьмемо до уваги, що $\prod_{j=1}^{\nu_i} q_{ij} \leq \prod_{j=1}^{\nu} q_{ij} \leq a_i^{\nu}$, $\prod_{j=1}^{\nu} q_{ij}^{1/\nu} + \prod_{j=1}^{\nu} R_{ij}^{1/\nu} \leq 1$. Тоді з (3.14) отримуємо:

$$\left(1-\left[\prod_{i=1}^{m}\left(1-\prod_{j=1}^{\nu_i} q_{ij}\right)\right]^{1/\nu}\right)^{\nu} \geq \left(1-\left[1-\prod_{i=1}^{m}\left(1-a_i^{\nu}\right)\right]^{1/\nu}\right)^{\nu} \geq \prod_{i=1}^{m}\left(1-a_i\right)^{\nu} =$$

$$=\left(\prod_{i=1}^{m}\left[1-\prod_{j=1}^{\nu} q_{ij}^{1/\nu}\right]\right)^{\nu} \geq \prod_{i=1}^{m}\left(\prod_{j==1}^{\nu} R_{ij}^{1/\nu}\right)^{\nu} = \prod_{i=1}^{m}\prod_{j=1}^{\nu} R_{ij} = \Pi_0 ,$$

або $1-\Pi_0^{1/\nu} \geq \left[1-\prod_{i=1}^{m}\left(1-\prod_{j=1}^{\nu_i} q_{ij}\right)\right]^{1/\nu} = \left(1-\widehat{P}_0\right)^{1/\nu}$, а значить $P_0 \geq 1-\left(\Pi_0^{1/\nu}\right)^{\nu}$, що й доводить теорему. Вона узагальнює відому нерівність Мінковського на випадок, коли $m>1$, оскільки при $m=1$ з (3.13) слідує, що $P=1-\prod_{i=1}^{\nu} q_i \geq 1-\left(1-\left(\prod_{i=1}^{\nu} R_i\right)^{\frac{1}{\nu}}\right)^{\nu}$, що характеризує систему з паралельним з'єднанням резервуючих елементів [84].

Зазначимо, що тут велике місце приділяється отриманню нових нерівностей. Це слід вважати природним, так як γ-нижня і γ-верхня межі y та $\overline{y}$ для функції $y=f\left(R_1,R_2...,R_m\right)$ від параметрів R_i повинні задовольняти нерівностям $P\left(\underline{y \leq y}\right) \geq \gamma$ та $P\left(\overline{y} \geq y\right) \geq \gamma$. Тому основним інструментом дослідження і доказів є метод нерівностей, що призводять до нетривіальних результатів.

Встановлена вище нерівність (3.13) дозволяє складне завдання знаходження γ-нижньої межі $\underline{\widehat{P}}_0$ для імовірності $\widehat{P}_0$ успішного функціонування системи (рис. 3.2) звести до більш простого завдання знаходження γ-нижньої межі $\underline{\Pi}_0$ для імовірності Π_0 успішного функціонування системи з послідовно з'єднаними v_m елементами (рис. 3.4).

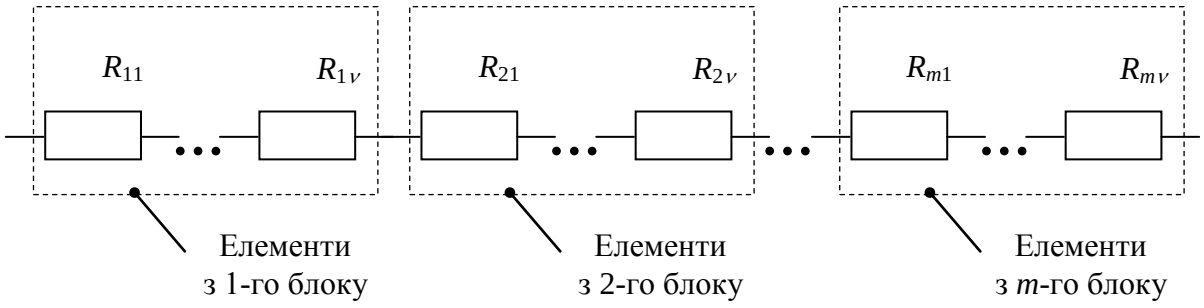


Рис. 3.4 – Приведена система з послідовно з'єднаними елементами, яка асоційована з системою рис. 3.2

При цьому $\Pi_0 = \prod_{i=1}^{m}\prod_{j=1}^{v} R_{ij} = R_{11}...R_{1v}R_{21}...R_{2v}...R_{m1}...R_{mv}$ – показник надійності системи рис. 3.4, яка асоційована з системою рис. 3.2. Для формування системи рис. 3.4 з кожного об'єкту системи рис. 3.2 вибирається $v = \min\limits_i v_i$ будь-яких елементів для яких є дані випробувань, що дозволяють знайти γ-нижню межу $\underline{\Pi}_0$ імовірності Π_0.

Теорема 2. Нехай елементи в системі рис. 3.2 різні, а події A_{ij} при $i = \overline{1,m}$, $j = \overline{1,v_i}$ – незалежні. Якщо за результатами випробувань v_m її елементів знайдена γ-нижня межа $\underline{\Pi}_0$ для імовірності Π_0 успішного функціонування системи рис. 3.4, то статистика

$$\underline{\widehat{P}}_0 = 1 - \left(1 - \underline{\Pi}_0^{1/v}\right)^v \qquad (3.15)$$

є нижньою межею для імовірності $\widehat{P}_0$ успішного функціонування системи з рис. 3.2.

Доведення. Використовуючи теорему 1 та враховуючи, що по умові теореми імовірність $P\left(\underline{\Pi}_0 > \Pi_0\right) \le 1-\gamma$, отримуємо: $P\left(\underline{\widehat{P}}_0 > \widehat{P}_0\right) \le P\left(\underline{\widehat{P}}_0 > 1-\left(\underline{\Pi}_0^{1/v}\right)^v\right) =$

$= P\left(1-\left(1-\Pi_0^{1/v}\right)^v > \left(1-\underline{\Pi}_0^{1/v}\right)^v\right) = P\left(\Pi_0 > \underline{\Pi}_0\right) \le 1-\gamma$, або $P\left(\underline{\widehat{P}}_0 \le \widehat{P}_0\right) \ge \gamma$. Теорема доведена.

Припустимо, що v_m елементів системи рис. 3.2, які входять в систему рис. 3.4, випробовуються (кожен) по схемі Бернуллі або по біноміальній схемі з зупинкою з реєстрацією значень випадкових величин n'_{ij}, де n'_{ij} дорівнює числу випробувань i-го об‘єкту до діставання першої відмови, якщо число відмов цього елементу $\tau_{ij} \ne 0$ та $\tau_{ij} = 0$. Якщо величини n'_{ij} при $i = \overline{1,m}$ та $j = \overline{1,v}$ незалежні, а n' – менша з них, то, згідно [89], статистика $\Pi_0 = \left(1-\gamma\right)^{1/n'}$ є γ-нижньою межею для Π_0. Звідси та на підставі теореми 3 (див. далі) робимо висновок про те, що в даній ситуації в якості γ-нижньої межі для імовірності $\widehat{P}_0$ успішного функціонування системи рис. 3.2 можна прийняти статистику

$$\underline{\widehat{P}}_0 = 1-\left(1-\left(1-\gamma\right)^{1/vn'}\right)^v. \tag{3.16}$$

При всіх відмовах $\tau_{ij} = 0$ дістаємо часткове значення:

$$\underline{\widehat{P}}_0 = 1-\left(1-\left(1-\gamma\right)^{1/vn}\right)^v, \tag{3.17}$$

де $n = \min\limits_{1\le i\le m}\min\limits_{1\le j\le v} n_{0j}$ – менше з чисел випробувань vm елементів системи рис. 3.2.

Якщо vm елементів системи рис. 3.2, що входять в систему рис. 3.4, випробовуються (кожен) n_{ij} раз по схемі Бернуллі з реєстрацією значень випадкових величин τ_{ij}, то у разі їх незалежності зі співвідношення (3.15) отримуємо ще один вираз для γ-нижньої межі:

$$\underline{\widehat{P}}_0 = 1-\left(1-f_2^{1/v}\left(n,\tau',\gamma\right)\right)^v, \tag{3.18}$$

де $\tau' = n\hat{q}$, n – менше з чисел vm випробувань елементів $\hat{q} = -\ln\hat{\Pi} \simeq 1-\hat{\Pi}$, $\hat{\Pi} = \prod_{i=1}^{m}\prod_{j=1}^{v}\left(1-\frac{\tau_{ij}}{n_{ij}}\right)$.

При всіх $\tau_{ij} = 0$ з (3.18) слідує формула (3.17). Для приблизних розрахунків можемо використовувати таку формулу:

$$\underline{\hat{P}}_0 \simeq 1-\left(1-\left(1-\hat{q}\right)^{1/v}\right)\left(1-\gamma\right)^{1/v(1-\hat{q})n}. \qquad (3.19)$$

Недоліком співвідношень (3.15)…(3.19) є те, що в них враховується лише менше значення v зі всіх чисел v_i, які можуть бути отримані для всіх елементів об‘єкту. У найбільш сприятливому випадку, коли v_i рівні, вони дають відмінні результати, але в найменш сприятливому випадку, тобто коли $v = 1$, можливе набуття занижених значень величини γ-нижньої межі для $\hat{P}_0$. У зв’язку з цим також представляють інтерес інші рішення даної задачі. Використовуючи матеріали, приведені в роботі [89], доведемо наступні нові твердження, які викладемо у вигляді теорем.

Теорема 3. Нехай для кожного з елементів системи рис. 3.2 за наслідками випробувань знаходяться γ-нижня $\underline{R}_{ij}$ та γ-верхня $\overline{R}_{ij}$ межі його успішного функціонування. Якщо $\underline{R}_*$ – менша з величин $\underline{R}_{ij}$, а $\overline{R}^*$ – більша з величин $\overline{R}_{ij}$, то статистика

$$\underline{\hat{P}}_0 = \prod_{ш=1}^{b}\left(1-\left(1-\underline{R}_*\right)^{v_i}\right) \qquad (3.20)$$

є γ-нижньою межею для імовірності $\hat{P}_0$, а статистика

$$\overline{\hat{P}}_0 = \prod_{ш-1}^{b}\left(1-\left(1-\overline{R}^*\right)^{v_i}\right) \qquad (3.21)$$

є γ-верхньою межею для $\hat{P}_0$.

Доведення. Нехай R_* – менша з імовірностей R_{ij}. Тоді

$$P\left(\underline{\hat{P}}_0 > \hat{P}_0\right) = P\left(\underline{\hat{P}}_0 > \prod_{i=1}^{m}\left(1-\prod_{j=1}^{v_i}\left(1-r_{ij}\right)\right)\right) \le P\left(\underline{\hat{P}}_0 > \prod_{i=1}^{m}\left(1-\left(1-R_*\right)^{v_i}\right)\right) = P(\prod_{i=1}^{m}\left(1-\left(1-\underline{R}_*\right)^{v_i}\right) >$$

$$> \prod_{i=1}^{m}\left(1-\left(1-R_*\right)^{v_i}\right)) = P\left(\underline{R}_* > R_* \triangleq R_{i'j'}\right),$$

де (i', j') – фиіксована пара індексів i та j, для якої $R_* = \min\limits_{i,j} R_{ij} = R_{i'j'}$.

Так як $\underline{R}_* \le \underline{R}_{i'j'}$, то з врахуванням того, що $\underline{R}_{i'j'}$ є γ-нижньою межею для $R_{i'j'}$, отримаємо: $P\left(\underline{\hat{P}}_0 > \hat{P}_0\right) \le P\left(\underline{R}_* > R_* = R_{i'j'}\right) \le P\left(\underline{R}_{i'j'} > R_{i'j'}\right) \le 1-\gamma$ або $P\left(\underline{\hat{P}}_0 \le \hat{P}\right) \ge \gamma$. Аналогічно: $P\left(\underline{\hat{P}}_0 < \hat{P}_0\right) \le P(\prod_{i=1}^{m}\left(1-\left(1-\overline{R}\right)\right) < (\prod_{i=1}^{m}\left(1-\left(1-R^*\right)^{v_i}\right) =$

$P\left(\overline{R}^* < R^* \triangleq R_{kl}\right) \le P\left(\overline{R}_{kl} < R_{kl}\right) \le 1-\gamma$ або $P\left(\overline{\hat{P}}_0 \ge \hat{P}_0\right) \ge \gamma$, де (k,l) – фіксована пара індексів i та j, для якої $R^* = R_{kl}$. Теорема доведена.

За рахунок «збереження» всіх чисел v_i (а не тільки меншого v з них) співвідношення (3.20) може давати кращі результати (3.15). При близьких v_i можливо зворотне. Важливою властивістю статистики (3.20) є те, що для її використання немає необхідності в допущенні про незалежність результатів випробувань.

Приклад 1. Нехай система рис. 3.2 складається з трьох об‘єктів з числами елементів $v_1 = 2$, $v_2 = 3$, $v_3 = 1$, кожен з яких випробовується по біноміальній схемі Бернуллі. Після випробувань отримані початкові дані у вигляді табл. 3.1.

Таблиця 3.1

Об‘єкт №1	Об‘єкт №2	Об‘єкт №3
$n_{11} = 10,\ \tau_{11} = 1$ $\tau_{12} = 20,\ \tau_{12} = 0$	$n_{21} = 10,\ \tau_{21} = 1$ $n_{22} = 40,\ \tau_{22} = 2$ $n_{23} = 10,\ \tau_{23} = 0$	$n_{31} = 50,\ \tau_{31} = 1$

З таблиць [90] за цими даними знаходимо значення γ-нижніх меж (при $\gamma = 0{,}90$: $\underline{R}_{11} = 0{,}66$; $\underline{R}_{12} = 0{,}89$; $\underline{R}_{21} = 0{,}66$; $\underline{R}_{22} = 0{,}87$; $\underline{R}_{23} = 0{,}79$;

$\underline{R}_{31} = 0,92$). Потрібно знайти значення γ-нижньої межі $\underline{\widehat{P}}_0$ для імовірності $\widehat{P}_0$ успішного функціонування системи в цілому.

Рішення. По формулі (3.20) з урахуванням того, що в даному випадку $\underline{R}_* = 0,66$ знаходимо: $\widehat{P}_0 = \left(1-0,34^2\right)\left(1-0,34^3\right)\left(1-0,34\right) = 0,54$.

Нехай тепер результати випробувань елементів незалежні. Тоді, враховуючи, що тут $v = 1$, цьому з кожного об‘єкту по $v = 1$ елементу (а саме: другий елемент з першого об‘єкту, третій елемент з другого і перший з третього) знайдемо значення γ-нижньої межі $\underline{\Pi}_0$ для імовірності $\Pi_0 = R_{12}R_{21}K_{31}$. Для цього, визначивши значення $\hat{\Pi}_0 = 1 - \dfrac{1}{50} = 0,98$ незміщеної оцінки для Π_0, із співвідношення (3.19) отримуємо $\underline{\widehat{P}}_0 = 0,98 \cdot 0,1^{\frac{1}{10 \cdot 0,98}} = 0,77 > 0,54$.

Проте при іншому виборі: одного першого елементів з кожного об‘єкту отримуємо інший результат, оскільки в цьому випадку $\hat{\Pi}_0 = \left(1-\dfrac{1}{10}\right)\times$, $\times\left(1-\dfrac{1}{10}\right)\left(1-\dfrac{1}{50}\right) = 0,79$, $\hat{q} = \left|\ln 0,79\right| = 0,24$, а значить (використовуємо формулу (3.18)) шукане значення буде дорівнювати:

$$\underline{\widehat{P}}_0 = \underline{\Pi}_0 = f_2\left(n, n\hat{q}, \gamma\right) = f_2\left(1–; 2,4; 0,90\right) = 0,51.$$

Примітки.

а) В умовах прикладу число $v = 1$. У зв’язку з цим вибиралося по одному елементу з кожного об‘єкту для знаходження γ-нижньої межі $\underline{\Pi}_0$. Через рівність $v = 1$ при цьому, згідно (3.18), виявлялося, що $\underline{\widehat{P}}_0 = \underline{\Pi}_0$. При $v > 1$ з кожного об‘єкту вибирається вже не по одному, а по v елементів $\left(v > 1\right)$.

б) Отримувані з (3.18) значення статистики $\underline{\widehat{P}}_0$ залежить від того, які саме v з v_i елементів в об‘єктах підлягають вибору. Цей вибір абсолютно довільний. У зв’язку з цим допустима оптимізаційна постановка наступного завдання: вибрати v з v_i елементів кожного об‘єкту так, щоб забезпечувався

максимум середнього значення величини $\underline{\widehat{P}}_0$ при обмеженнях на вартість і час проведення випробувань.

Отримаємо ще одну формулу, що дозволяє знайти γ-нижню межу для $\widehat{P}_0$.

Визначення. Нехай θ – невідома константа, яка підлягає оцінюванню по результатах $\omega \in \Omega$ випробувань, де Ω – сукупність всіх результатів ω. Статистика $\underline{\theta}_\gamma = \underline{\theta}_\gamma(\omega)$, для якої виконується нерівність $P(\theta_\gamma \le \theta) \ge \gamma$ називається *правильною* γ-нижньою межею для θ, якщо $\theta \in (0,1]$, її функція розподілу $P(\theta_\gamma \le c) = F(\theta, \gamma, c), c \in [0,1]$ містить параметр θ і правильно залежить від нього. Це означає, що відображення q, що задається за допомогою співвідношення $q(t) = 1 - F(t, \gamma, c)$ або $q(t) = 1 - \tilde{F}(t, \gamma, c) \ge 1 - F(t, \gamma, c)$, задовольняє умовам а) та б), а саме:

а) Функція $q(t)$ має похідну $q'(t) > 0$ на $(y,1)$, визначена і безперервна на $[y,1]$, де $y \in (0,1)$, причому $q(1) = 1$, а добуток

$$\Psi_k(t) q(t) q^k \left(\frac{y}{t} \right)^{1/k} \tag{3.22}$$

має на $(y,1)$ єдиний екстремум або постійний та рівний $q(y)$.

б) При $t = c$ виконується співвідношення $\forall t \in (0,1): 1 - F(t, \gamma, t) \le 1 - \gamma, \gamma \in (0,1)$. Вважається, що при даному ω значення $\underline{\theta}^k_{\gamma_k}, \gamma_k = 1 - (1-\gamma)^{1/k}, k = \overline{1,m}$ утворюють незростаючу послідовність, так що

$$\forall k \in I_m = \{1, 2, ..., m\} : \underline{\theta}^m_{\gamma_m} \le \underline{\theta}^k_{\gamma_k}, \underline{\theta}^{k+1}_{\gamma_{k+1}} \le \underline{\theta}^k_{\gamma_k}. \tag{3.23}$$

Сукупність всіх функцій $F(\theta, \gamma, c)$, для яких вказані умови виконуються, позначимо буквою F_0. Загальна назва для ідеальної і правильної γ-межі – монотонна 0-нижня межа.

В [86, 87] показано, що клас F_0 не порожній. Зокрема статистика $\underline{R} = f_2(n, \tau, \gamma)$ має функцію розподілу з F, тобто γ-нижня межа Клопера-Пірсона є правильною.

Покажемо, що клас F описує більше типових γ-нижніх меж. У цьому напрямі справедливий наступний результат.

Теорема 4. Статистика

$$\underline{R}_\gamma = (1-\gamma)^{1/n'}, \tag{3.24}$$

що є γ-нижньою межею для параметра R біноміального розподілу (див. [86] та ін.), де n' – число випробувань до першої відмови при їх числі $\tau \neq 0$ та $n' = n$ при $\tau = 0$, є правильною і одночасно ідеальною γ-нижньою межею R.

Доведення. Згідно до [89], справедливе співвідношення:

$$P\left(\underline{R}_\gamma > c\right) = P\left(n' > l = \frac{\ln(1-\gamma)}{\ln c}\right) = 1 - P\left(n' \le l\right) = 1 - \frac{1}{S_0}\sum_{k=0}^{[l]} R^k (1-R) = 1 - F\left(R,\gamma,c\right) =$$

$$= 1 - \frac{1-R}{S_0}\frac{1-R^{[l]+1}}{1-R} = 1 - \frac{1-R^{[l]+1}}{1-R^{n+1}} \le 1 - \left(1-R^{[l]+1}\right) = R^{[l]+1} \le R^l,$$

де $S_0 = \sum_{k=0}^{n} R^k (1-R) = 1-R^{n+1}$, $l = \frac{\ln(1-\gamma)}{\ln c}$, $(1-\gamma)^{1/n'} \le (1-\gamma)^{1/n} = c' \Rightarrow 1 - F\left(R,\gamma,c\right) = 0$.

При $c > c'$ функція $q(t) = 1 - F\left(t,\gamma,c\right) = t^{[l]+1}$, $l = \frac{\ln(1-\gamma)}{\ln c}$, має похідну $q'(t)\left([l]+1\right)t^{[l]} > 0$, визначена і безперервна на $[0,1]$, причому $q(1) = 1$, а $\max\limits_{x_1 x_2 \ldots x_m = y} \prod\limits_{i=1}^{m} q\left(x_i\right) = y^{[l]+1} = \max\limits_{1 \le k \le m} q^k\left(y^{1/k}\right)$. При цьому послідовність $\underline{R}^k_{\gamma_k} = (1-\gamma)^{1/n}$, $k = 1,2,\ldots,m$ є постійною для $k \ge 1$. Нарешті $\forall t \in (0,1)$: $1 - F\left(t,\gamma,t\right) = 1 - \left(1 - t^{[l]+1}\right) =$

$= t^{[l]+1} \le t^l \equiv 1-\gamma$ оскільки тут $l = \frac{\ln(1-\gamma)}{\ln t}$. Теорема доведена.

Т.ч. ми маємо два приклади правильних γ-нижніх меж: статистика $R = f_2\left(n,\tau,\gamma\right)$ Клопера-Пірсона і статистика (3.24), яка запропонована в [86, 87]. Обидві вони є γ-нижніми межами для параметра R біноміального розподілу). Цікаво відзначити, що γ-нижня межа (3.24) є прикордонною для правильних та ідеальних γ-нижніх меж, так як послідовність $\underline{R}^k_{\gamma_k} = \left(1-\gamma_k\right)^{k/n'} = (1-\gamma)^{1/n'}$ постійна, тобто не зростає і не убуває по $k \ge 1$. Це означає, що теорема 4 є

прикладом статистики, яка є для параметра R біноміального розподілу одночасно правильною та ідеальною. Для отримання інших ідеальних γ-меж представимо наступний допоміжний результат.

Лема. При $t\in(0,1]$, $x\in[0,1]$ та $v\geq 1$ виконується нерівність

$$\left(1-\left(1-x^t\right)^v\right)^{1/t}\geq 1-(1-x)^v \tag{3.25}$$

Знак рівності досягається при $v=1$ та при $t=1$.

Доведення. Запишемо дану нерівність у вигляді $1-\left(1-x^t\right)^v\geq\left(1-(1-x)^v\right)^t$,

$f(t)=\left(1-x^t\right)^v\leq\ \leq\left(1-(1-x)^v\right)^t=q(t)$ або $\dfrac{f(t)}{q(t)}=\dfrac{\left(1-x^t\right)^v}{1-\left(1-(1-x)^v\right)^t}\leq 1$. Згідно [91], f, q та $\dfrac{f'}{q'}$ – позитивні зростаючі функції. Тоді при $f(0)=q(0)=0$ функція $\dfrac{f}{q}$ зростає для $t>0$. У нашому випадку $f(0)=q(0)=0$, причому f та q позитивні і зростають по $t>0$, оскільки $f'(t)=\ =-v\left(1-x^t\right)^{v-1}x^t\ln x>0$. При цьому відношення похідних $\dfrac{f'(t)}{q'(t)}=\dfrac{\left(1-x^t\right)^{v-1}}{\left(1-(1-x)^v\right)^t}\dfrac{vx^t\ln x}{\ln\left(1-(1-x)^v\right)}$ зростає для $t>0$ та $v>1$, оскільки функція $\left(1-x^t\right)^{v-1}$ за цих умов зростає по $t>0$, тоді як функція $\left(1-(1-x)^v\right)^t$ убуває по $t>0$.

З урахуванням викладеного можемо зробити висновок, що $\dfrac{t}{q}$ зростає для $t>0$, а значить $t<1\Rightarrow\dfrac{f(t)}{q(t)}<\dfrac{f(1)}{q(1)}=1$, що і доводить лему.

Теорема 5. Нехай у виразі $\underline{\widehat{P}}_\gamma=1-\left(1-\underline{R}_\gamma\right)^v$, що дозволяє знайти γ-нижню межу $\underline{\widehat{P}}_\gamma$ для імовірності $\widehat{P}=1-(1-R)^v$, статистика $\underline{R}_\gamma$ є ідеальною

γ-нижньою межею для імовірності R. Тоді статистика $\underline{\widehat{P}}_\gamma$ є ідеальною γ-нижньою межею для $\widehat{P}$.

Доведення. З формули $\widehat{P}=1-(1-R)^v$ слідує, що $R=1-\left(1-\widehat{P}\right)^{1/v}$, а значить $\left(\underline{R}_\gamma > c'\right)=P\left(\widehat{P}_\gamma > c\right)=1-\overset{0}{F}=P\left(\underline{R}_\gamma > c'\right)=1-F\left(R,\gamma,c'\right)$, де $c'=1-(1-c)^{1/v}$, а $\overset{0}{F}$ та F – функції розподілу $\underline{\widehat{P}}_\gamma$ та $\underline{R}_\gamma$. Далі слід встановити, що $F\in\widehat{P}_0 \Rightarrow \overset{0}{F}\in\widehat{P}_0$. З цією метою розглянемо функцію $\overset{0}{q}(t)=1-\overset{0}{F}(t,\gamma,c)=$ $=1-F\left(t,\gamma,c'\right)=q\left(1-(1-t)^{1/v}\right)=q\left(Z_t\right)$, де $Z_t=1-(1-t)^{1/v}$. Оскільки по умові теореми функція q визначена і направлена на $[y,1]\subset(0,1)$, $q^{(1)}=1$ та $q'(t)>0$, причому $Z_t'>0$ на $(0,1)$, то цими ж властивостями володіє і функція $\overset{0}{q}(t)$. Крім того оскільки по умові теореми $\underline{R}_{\gamma_{k+1}}^{k+1}\geq\underline{R}_{\gamma_k}^{k}$, $k\geq 1$, то позначаючи $t=\dfrac{k}{k+1}$, з (3.25) отримуємо:

$$\underline{\widehat{P}}_{\gamma_{k+1}}^{k+1}=\left(1-\left(1-\underline{R}_{\gamma_{k+1}}\right)^v\right)^{k+1}=\left(1-\left(1-\underline{R}_{\gamma_{k+1}}^{(k+1)\frac{1}{k+1}}\right)^v\right)^{k+1}\geq\left(1-\left(1-\underline{R}_{\gamma_k}^{\frac{k}{k+1}}\right)^v\right)^{k+1}=$$

$$=\left(1-\left(1-\underline{R}_{\gamma_k}^{t}\right)^v\right)^{\frac{1}{t}k}\geq\left(1-\left(1-\underline{R}_{\gamma_k}\right)^v\right)^{k},$$

або $\underline{R}_{\gamma_{k+1}}^{k+1}\geq\underline{R}_{\gamma_k}^{k}\Rightarrow\underline{\widehat{P}}_{\gamma_{k+1}}^{k+1}\geq\underline{\widehat{P}}_{\gamma_k}^{k}$. Теорема доведена.

Аналогічно викладеному встановлюється наступний результат.

Теорема 6. Нехай у виразі $\underline{\widehat{P}}_\gamma=1-\left(1-\Pi_\gamma^{1/v}\right)^v$, який згідно викладеного дозволяє знайти γ-нижню межу $\underline{\widehat{P}}_\gamma$ для імовірності $\widehat{P}=1-(1-R_1)(1-R_2)...(1-R_v)$, статистика $\underline{\Pi}_\gamma$ є ідеальною. Тоді статистика $\underline{\widehat{P}}_\gamma$ є ідеальною γ-нижньою межею імовірності $\widehat{P}$.

Теорему 6 можна довести аналогічно теоремі 5.

Приведені теореми мають важливе значення для теорії дослідження автоматичних систем з послідовно-паралельним з’єднанням елементів та мо-

жуть бути використані при розгляді та аналізі багатьох аспектів інтервального оцінювання робочих параметрів при випробуваннях надійності автоматичних систем однократного використання. Для отримання загального результату по зазначених питаннях потребує доказу наступна теорема:

Теорема. Нехай кожен з елементів $\nu_1 + \nu_2 + ... + \nu_m$ системи з послідовно-паралельним з'єднанням резервуючих елементів випробовується по біноміальному плану з зупинкою. Нехай по результатах випробувань реєструються значення випадкових величин $n_{ij}^{/}, i = \overline{1,m}, \ j = \overline{1,\nu_i}$. При цьому $n_{ij}^{/}$ – кількість випробувань до отримання першої відмови j-го елемента з i-го об'єкту (якщо число r_{ij} його відмов не дорівнює нулю) та $n_{ij}^{/} = n_{ij}$ при $r_{ij} = 0$, де n_{ij} – встановлений обсяг випробувань вказаного елемента. Тоді, якщо величини $n_{ij}^{/}$ при $i = \overline{1,m}$ та $j = \overline{1,\nu_i}$ є незалежними, в якості γ-нижньої межі $\underline{P_0}$ для імовірності $P_0 = \prod_{i=1}^{m} P_i$ (де $P_i = 1 - \prod_{j=1}^{\nu_i} \left(1 - R_{ij}\right)$) успішного функціонування автоматичної системи (рис. 3.2) з різноманітними елементами можна прийняти статистику $\underline{P_0} = \min \underline{P_{i\gamma}} = 1 - \max_{1 \le i \le m} \left(1 - \left(1 - \gamma\right)^{\frac{1}{n_i \nu_i}} \right)^{\nu_i}$, де $n_i^{/} = \min_{1 \le j \le \nu_i} n_{ij}^{/}$ – менша з величин $n_{ij}^{/}$ в j-му об'єкті.

Доказ приведеної теореми є перспективою подальших досліджень щодо надійності автоматичних банківських інформаційних систем з послідовно-паралельним з'єднанням резервуючих елементів.

3.4. Регуляризований розв'язок одномірного інтегрального рівняння Фредгольма I роду в умовах існування некоректних задач

В умовах невизначеності інформації, яка може бути отримана автоматичними системами моніторингу інформаційного простору (АСМІП) з метою прийняття відповідних управлінських рішень, вплив достовірності первинних даних про стан об'єктів чи процесів на їх ефективність є достатньо істот-

ним. Відповідно, першочерговим завданням для інформаційно-комунікаційних систем (ІКС), які обслуговують галузь економіки, бізнесу та фінансів, та діють в умовах невизначеності первинної інформації, є розробка методів перетворення та відновлення інформації. Така задача, як правило, в сучасних ІКС розв'язується в рамках їхнього технічного, інформаційного та програмно-математичного забезпечення (ПМЗ). АСМІП, як приклад, відносяться саме до систем ПМЗ. На сьогодні АСМІП – це достатньо широкий клас систем з розширеною функціональністю основним завданням яких є забезпечення процесу спостереження та реєстрацію даних про явища та об'єкти або зміну інформації про їх стан на інтервалах часу, що нерозривно примикають один до одного протягом яких значення даних істотно не змінюються. Саме останнє зауваження щодо неістотної зміни інформації та наслідків, які можуть звідси витікати, є підставою для того, щоб віднести їх до типу некоректних задач.

Важливою проблемою моніторингу інформаційного простору галузі економіки, бізнесу та фінансів є розв'язання математичних задач відновлення даних та інтерпретації результатів спостережень, ефективне рішення яких дозволяє підвищити точність систем спостереження. Автоматична корекція похибок в даних, які отримуються АСМІП, створює можливості щодо підвищення розрізнюючої здатності засобів спостереження, вимірювання та контролю, а це, в свою чергу, дозволить реєструвати найнезначніші зміни об'єктів моніторингу. Підвищення розрізнюючої здатності та забезпечення точності математичних залежностей вимагає розв'язання задачі відновлення інформації.

Як правило, у прямих завданнях математичної фізики дослідники прагнуть знайти достатньо точні функції, які описують різні фізичні явища. При цьому властивості середовища, які представляються у вигляді коефіцієнтів рівнянь, а також початковий стан процесу при нестаціонарних випадках або його властивості, встановлені на межі достовірності даних, вважаються відомими. Відмітимо, що грань достовірності, в загальному випадку, виникає у разі обмеження області досліджень та/або при дослідженнях стаціонарних випадків, де відсутність динаміки не дозволяє встановити точні межі відхилення досліджуваних величин [92].

Як показав аналіз праць головного наукового співробітника лабораторії хвильових процесів Інституту механіки Сибірського відділення РАН проф.

Кабанихіна С.І. (наприклад, [93]), положення щодо недостовірності даних, отриманих при дослідженні фізичних процесів, та, як наслідок, виникнення проблеми рішення некоректних задач відновлення даних, можна розповсюдити на інформаційні середовища та на ті явища, які в них досліджуються. Проте саме властивості середовища у силу його надзвичайної фізично-інформаційної складності на практиці часто є невідомими. А це означає, що необхідно ставити та вирішувати зворотні завдання в яких потрібно визначати або коефіцієнти рівнянь, або невідомі початкові та/або граничні умови, або місцеположення, межі та інші властивості фізичних та інформаційних просторів в яких відбуваються досліджувані процеси. Ці завдання в більшості випадків некоректні, тобто в них порушена хоч би одна з трьох властивостей коректності (див., наприклад, [94, 95]). Щодо інформаційних середовищ, то шуканими коефіцієнтами рівнянь є, як правило, достовірність інформації у сенсі порушення її смислового значення або достовірність даних у сенсі надійного відновлення електричних сигналів та ін. Крім того, якщо розглядати сучасні АСМІП (наприклад, моніторинг простору пошуковими роботами), то дуже часто в зворотних завданнях потрібно знайти місцеположення заданого об’єкта, форму, структуру та вид інформаційних включень, дефекти інформаційного середовища (мереж), джерел інформації (сайтів, інформаційних сторінок) і т.д. Недивно, що при такому широкому наборі додатків, теорія зворотних та некоректних завдань з моменту своєї появи стала однією з областей сучасної науки, які найстрімкіше розвиваються.

На поточний час розроблений широкий спектр різних підходів до розв’язання некоректних задач. Методи розв’язання некоректних задач отримали інтенсивний розвиток в 60-ті роки XX ст. Основою для досліджень в даній області є праці наукової школи А.М. Тихонова, який створив математичну теорію некоректно поставлених задач. Сюди належать метод регуляризації А.М. Тихонова, метод заміни М.М. Лаврентьєва, метод підбору та квазірозв’язку В.К. Іванова та інші методи. Розроблені також методи ітеративної, статистичної, локальної, дискриптивної регуляризації, субоптимальної фільтрації, розв’язання на компакті та ін. Іноземні розробки представлені методами оптимальної фільтрації Калмана-Б’юсі та Вінера, методами керованої

лінійної фільтрації Бейкуса-Гільберта та ін. Зазначені методи відрізняються точністю отриманих рішень, вимогами до первинних даних, кількістю додаткової інформації, яка потрібна для їх реалізації та іншими чинниками.

Виходячи зі сказаного, однією з частин загальної проблеми може бути вирішення інтегрального рівняння типу згортки на основі застосування методу перетворення Фур'є. При цьому під зазначеним рівнянням буде розумітися одновимірне інтегральне рівняння Фредгольма першого роду. При рішенні ***вперше береться до уваги існування некоректних завдань***. Враховується, що метод перетворення Фур'є буде оперувати тільки з векторами.

Слід відзначити, що для стійкого розв'язання інтегральних рівнянь I роду, крім вище зазначених методів регуляризації Тихонова та квазірозв'язків Іванова, застосовуються методи детерміністської регуляризації, методи регуляризації Лаврентьєва та Денисова, метод «занурення» Бакушинського, метод максимальної ентропії Берга, методи ітеративної регуляризації Фрідмана та Морозова, метод локальної регуляризації Арсеніна, метод регуляризуючих алгоритмів Бакушинського, метод пошуку розв'язку «на компакті», метод дескриптивної регуляризації Морозова та ін.

Постановкою завдання та метою дослідження в поточному підрозділі є підвищення ефективності щодо використання ресурсів пам'яті, яка задіяна в АСМІП, та часу рішення задач систематичного збору та обробки інформації, яка може бути використана для поліпшення процесу ухвалення рішення, а також, побічно, як інструмент зворотного зв'язку в цілях здійснення проектів, оцінки програм, вироблення політики та ін., на основі регуляризованого розв'язку одновимірного інтегрального рівняння Фредгольма першого роду в умовах існування некоректних задач.

У 1943 році Тихонов А.М. запропонував розглядати некоректно поставлені задачі шляхом апріорного звуження класу можливих розв'язків. *Метод регуляризації Тихонова А.М.* (МРТ) − це глобальна ідея граничного переходу до точного розв'язку при істотно малих значеннях основних вхідних параметрів задачі. МРТ є подальшим розвитком методу найменших квадратів Гауса (МНК) та методу псевдооберненої матриці Мура-Пенроуза (МПОМ). При

рішенні за першим методом отримується псевдорозв'язок, а за другим – нормальний.

Відмінність умовної коректності, введеної Тихоновим А.М., від класичної коректності по Адамару полягає у введенні множини коректності Y_K, яка істотно звужує клас можливих розв'язків. Т.ч., задача розв'язання рівняння може бути названа *умовно коректною* або *коректною по Тихонову*, якщо апріорі відомо, що:

– розв'язок існує та належить деякій заданій множині Y_K: $y \in Y_K \subset Y$ (де Y_K названа *множиною коректності*);

– розв'язок у єдиний в Y_K;

– малим змінам $\tilde{f}$ відповідають малі зміни розв'язку в $y \in Y_K$.

Тихонов А.М. на основі ідеї умовної коректності також розробив принципово новий метод розв'язання умовно коректних задач. Його суть полягає в тому, що якщо на множині Y розв'язок неєдиний або нестійкий, то поле пошуку обмежується множиною $Y_K \subset Y$ за допомогою апріорних відомостей про шуканий розв'язок і про похибки вихідних даних, наприклад, введенням додаткових характеристик, названих функціоналом $T(f)$, для розрізнення та підбору розв'язків необхідної якості. Відомості про похибки вихідних даних включають верхню оцінку похибок $\delta_y \geq \rho_y(\tilde{f}, f)$.

Перед тим, як ввести поняття про регуляризучий оператор, відзначимо, що математично під оберненою задачею відновлення інформації про стан інформаційного простору, який є предметом дослідження в АСМІП, будемо розуміти задачу, яка має на меті знаходження функції $y(s)$ по функції $f(x)$, яка може бути отримати з попереднього експерименту або зі спостережень, які знаходяться у базі даних, з рівняння вигляду:

$$f(x) = A[x, y(s)] \tag{3.26}$$

де A – деякий оператор, який встановлює причинно-наслідковий зв'язок між $y(s)$ та $f(x)$.

Як правило, вираз (3.26) має вигляд операторного рівняння:

$$f = Ay. \tag{3.27}$$

Означення. Для рівняння (3.27) в області значення f оператор $R(f,\delta)$ будемо називати регуляризуючим якщо:

1) $R(f,\delta)$ визначений для всіх $\tilde{f} \in F$ і $0 \le \delta \le \delta_0$ (δ_0 − деяке граничне значення при якому $R(f,\delta)$ залишається регуляризуючим оператором);

2) для будь-якого $\varepsilon > 0$ існує $\varepsilon(\delta)$ таке, що якщо $\rho_F\left(\tilde{f}, f\right) \le \delta \le \delta(\varepsilon)$, то $\rho_y(\tilde{y}_\delta, y) \le \varepsilon$, де $\tilde{y}_\delta = R\left(\tilde{f}_\delta, \delta\right)$, а y − точний розв'язок (тобто розв'язок $\tilde{y}_\delta = R\left(\tilde{f}_\delta, \delta\right)$) повинен бути стійким). При цьому при $\delta \to 0$ розв'язок має $\varepsilon \to 0$, тобто наближений розв'язок $\tilde{y}_\delta$, який надає регуляризуючий алгоритм, повинен переходити при $\delta \to 0$ 0 у точний розв'язок y.

У задачі на відшукання екстремуму функціоналу $T(f)$, що включає апріорну інформацію про розв'язок, забезпечується трансформація вихідної моделі системи спостереження A до моделі A_T, тобто операція регуляризації. При цьому A_T у тому чи іншому вигляді включає оператор A, але цей оператор не є в строгому значенні моделлю системи спостереження внаслідок порушення структурної відповідності об'єкту, що моделюється, та утруднень у фізичній інтерпретації елементів A_T, що відрізняють його від A. Оператор A_T моделює гіпотетичну фізичну систему, подібну до розглянутої у [95] системи спостереження за результатами функціонування, але яка відрізняється елементами структури.

В операторному рівнянні (3.27) для f та A відомі їхні наближення, такі що

$$\left\| \tilde{f} - f \right\|_{L_2} \le \delta, \left\| \tilde{A} - \hat{O} \right\| \le \xi \tag{3.28}$$

з верхніми оцінками правої частини та оператора, тобто розв'язується рівняння $\tilde{A}\tilde{y} = \tilde{f}$, $\tilde{y} \in L_2$, $\tilde{f} \in L_2$. МРТ має на увазі виконання двох умови:

1) умова мінімізації *нев'язки* $\min\limits_y \left\| A_y - f \right\|_{l_2}^2$, як у МНК;

2) умова мінімізації норми розв'язання типу (3.28), як у МПОМ.

Це являється задачею умовної мінімізації. Вона розв'язується методом невизначених множників Лагранжа, а саме:

$$\min_{y}\left\{\left\|A_y - f\right\|_{l_2}^2 + \alpha\left\|y\right\|_{l_2}^2\right\}, \tag{3.29}$$

де $\alpha > 0$ − параметр регуляризації, який виконує роль невизначеного множника Лагранжа.

Викладене має на увазі застосування згладжуючого функціоналу, який включає функціонал МНК – $\left\|A_y - f\right\|_{l_2}^2$, та стабілізуючого функціоналу $\Omega(y) = \left\|y\right\|_{L_2}^2$. Перший з функціоналів враховує похибки спостережень, а другий містить інформацію про розв'язок і може уточнюватися в залежності від способів ймовірного використання отриманого розв'язку, наприклад, інтегрування, диференціювання, розпізнавання.

З умови (3.29) витікає рівняння Тихонова:

$$(\alpha E + A^* A)Y_\alpha = A^* f, \tag{3.30}$$

де E − одиничний оператор $Ey = y$. Отже замість рівняння I роду отримане рівняння II роду (3.30).

Якщо в (3.29) та (3.30) $\alpha = 0$, то метод регуляризації Тихонова переходить у МНК з украй нестійким розв'язком, але мінімальною нев'язкою $\left\|Ay - f\right\|^2$. Зі збільшенням α розв'язок стає згладженим та стійкішим, тобто зменшується норма розв'язку $\left\|y_a\right\|^2$, але збільшується нев'язка. Отже, при деякому помірному α розв'язок y_α буде мати як помірну гладкість, так і помірну нев'язку.

Якщо δ, $\varepsilon \to 0$, то $\alpha \to 0$ і, відповідно, $y_\alpha = \lim_{\alpha\to 0}(\alpha E + A^* A)^{-1} A^* f = A^{+f}$. Це значить, що розв'язок y_α переходить у нормальний псевдорозв'язок. У такий спосіб МРТ є узагальненням МНК та МПОМ.

МРТ стійкий, тобто виконується 3-й пункт коректності по Адамару [95] і ця стійкість обумовлена наступними обставинами:

Оператор A^*A в (3.30) є додатньо визначеним, тому всі його власні значення дійсні та додатні, тобто $\lambda_i(A^*A) \geq 0$, причому $\lambda(A^*A)_{\min} = 0$. Наявність доданку aE в (3.30) збільшує всі $\lambda_i(A^*A)$ на α, тому $\alpha E + \lambda(A^*A)_{\min} = \alpha$. Внаслідок цього, оператор $\alpha E + A^*A$ стає оборотним, норма оберненого оператора – $\left\|(\alpha E + A^*A)^{-1}\right\| = 1/\alpha \neq \infty$, і, як наслідок, задача стає стійкою. Розв'язком (3.30) є: $y_\alpha = (\alpha E + A^*A)^{-1} A^* f$.

Метод Тихонова (МТ) спирається на поняття регуляризуючого оператора. Оператор $\Re(f, \delta_f)$ називається регуляризуючим для рівняння (3.28) в області впливу f при виконанні двох умов:

1) $\Re(f, \delta_f)$ визначений для будь-яких $f \in F$ та $\delta_f \in (0, \delta_{\max})$ так, що $\tilde{y} = \Re(f, \delta_f)$;

2) для будь-якого $\delta_y > 0$ існує таке $\delta_y(\delta_f)$, що якщо при $\rho_f(\tilde{f}, f) \leq \delta_f \leq$ $\leq \delta_f(\delta_y)$, то $\rho_y(\tilde{y}, y) \leq \delta_y$, тобто наближений розв'язок $\tilde{y}$, утворений регуляризуючим оператором $\Re$ при $\delta_f \to 0$ переходить у точний розв'язок y.

Т.ч., поняття регуляризуючого оператора за умови $\delta_f \to 0$ узагальнює поняття оберненого оператора.

Базуючись на викладеному, озглянемо окремий випадок регуляризованого розв'язку одновимірного інтегрального рівняння Фредгольма (ІРФ) I роду в умовах існування некоректних задач − рівняння типу згортки одномірне та двомірне.

Якщо рівняння загального вигляду (3.28) при його числовому розв'язку методом квадратур вимагає розміщення в комп'ютерній пам'яті матриці системи лінійних алгебраїчних рівнянь (СЛАР) і це обмежує можливості методу, то для розв'язання одномірного рівняння типу згортки можливе застосування методу перетворення Фур'є, який оперує лише з векторами, що істотно роз-

ширює можливості методу стосовно використання пам'яті та часу розв'язання. Це ще більш характерно для двовимірного рівняння.

ІРФ І роду типу згортки має вигляд:

$$Ay = \int_{-\infty}^{\infty} K(x-s)y(s)ds = f(x), -\infty < x < \infty.$$

Щодо нього в МРТ розв'язок знаходиться з умови мінімуму згладжуючого функціоналу:

$$\int_{-\infty}^{\infty} K(x-s)y(s)ds = f(x), -\infty < x < \infty, \quad (3.31)$$

де $M(\omega) = |\omega|^{2q}$ – регуляризатор q-го порядку, причому $q \geq 0$ – порядок регулярзації, що задається, наприклад, $q = 1$.

З умови (3.31) випливає наступний вираз для регуляризованого розв'язку:

$$y_\alpha(s) = \frac{1}{2\pi} \int_{-\infty}^{\infty} \frac{\lambda(-\omega)F(\omega)}{L(\omega) + \alpha M(\omega)} e^{-i\omega s} d\omega, \quad (3.32)$$

де:

$$L(\omega) = |\lambda(\omega)|^2 = \lambda(\omega)\lambda(-\omega) = \mathrm{Re}^2\lambda(\omega) + \mathrm{Im}^2\lambda(\omega), \; y_\alpha(s) = \int_{-\infty}^{\infty} R_\alpha(s-x) f(x) dx, \quad (3.33)$$

$$R_\alpha(s) = \frac{1}{2\pi} \int_{-\infty}^{\infty} \frac{\lambda(-\omega)}{L(\omega) + \alpha M(\omega)} e^{-i\omega s} d\omega \quad (3.34)$$

У розв'язку (3.32) за рахунок $\alpha M(\omega)$ підінтегральна функція наближається до нуля $\omega| \to \infty$, тобто доданок $\alpha M(\omega)$ зменшує реакцію високих гармонік на похибку вихідних даних, причому зменшує тим інтенсивніше, чим більше значення α та q. При цьому, чим більшим є q, тим більш істотно зменшуються високі гармоніки в розв'язку в порівнянні з низькими. Параметр α визначає глобальне зменшення: з його збільшенням інтенсивніше зменшуються всі гармоніки. Щодо параметра регуляризації α, то способи

його вибору такі ж, що й для рівняння (3.28), тобто способи нев'язки, підбору та ін.

Розроблено ряд числових алгоритмів одержання розв'язку $y_\alpha(s)$ [96]. Усі вони засновані на заміні інтегралів у (3.32)…(3.34) кінцевими (скінченими) сумами (по формулах прямокутників або трапецій), і, тим самим, на переході від нескінченного перетворення Фур'є до його дискретного представлення та використанні алгоритму швидкого перетворення Фур'є.

Розв'язання ІРФ І роду за допомогою перетворення Фур'є виправдано лише в деяких випадках, тобто лише тоді, якщо розв'язується рівняння типу згортки. Часто навіть для рівняння типу згортки розв'язання шукається на обмеженому інтервалі значень аргументу, внаслідок чого носій ядра обмежується і різницеве ядро рівняння типу згортки втрачає властивість стаціонарності (різницевості), і, як наслідок, тому метод Фур'є-перетворень стає непридатним.

При числовій реалізації МТ є більш гнучким і має більше можливостей для варіювання регуляризуючих параметрів. При розв'язанні задачі отримання наближеного розв'язку рівняння, яке стійке до незначних змін правої частини, МРТ зводиться до знаходження регуляризуючих операторів та до визначення параметру регуляризації за інформацією про задачу. Відомості про це є у достатній кількості літературних джерел (див., наприклад, список літератури у [95]). МТ також вимагає мінімуму апріорної інформації про задачу. Практично використовується лише інформація про характер гладкості розв'язку та про те, що відновлюваний сигнал заданий на відрізку $[\alpha,b]$.

У рамках МТ найбільш ефективним способом підвищення точності розв'язку є збільшення інформативності правої частини, що пов'язано з помірним зростанням кількості обчислень. Для мінімізації отриманих вище оцінок, точність представлення шуканої функції бажано збільшувати за рахунок скорочення інтервалу $[\alpha,b]$ на якому шукається розв'язок, а також шляхом оптимізації нерівномірного кроку дискретизації по змінній s. При дослідженні точності варіюються такі регуляризуючі параметри, як α, сітка дискретного

представлення правої частини та область її визначення; аналогічна сітка шуканого розв'язку.

У [97] Морозовим В.А. дана оцінка методу, смислове значення якої полягає в тому, що МРТ є достатньо легким щодо його реалізації на практиці у зв'язку з тим, що він не вимагає фактичного завдання множини M у якій міститься шуканий розв'язок рівняння (3.28). Там же відмічено, що основними труднощами застосування методу є формулювання алгоритмічних принципів вибору параметра регуляризації α. Крім того, Морозов В.А. в [98] вказав, що значимість роботи [99], в якій вперше був викладений МРТ, важко переоцінити. Ця робота послужила поштовхом для виконання цілого ряду досліджень іншими вченими у багатьох областях математичного аналізу та природознавства, включаючи спектроскопію, електронну мікроскопію, ідентифікацію в системах автоматичного регулювання, гравіметрію, оптику, ядерну фізику, фізику плазми, метеорологію, автоматизацію наукових досліджень та ряд інших розділів науки і техніки.

З врахуванням сказаного, щодо ІРФ І роду

$$Ay \equiv \int_{\alpha}^{b} K(x,s)\,y(s)\,ds = f(x),\ c \le x \le d, \tag{3.35}$$

співвідношення $(\alpha E + A^{*}A)\,y_a = A^{*}f$ набуває вигляду ІРФ ІІ роду з додатньо визначеним ядром: $\alpha y(t) + \int_{\alpha}^{b} R(t,s)\,y_a(s)\,ds = f(x),\ \alpha \le t \le b$, де:

$$R(t,s) = R(s,t) = \int_{c}^{d} K(x,t)\,K(x,s)\,ds, \tag{3.36}$$

$$F(t) = \int_{c}^{d} K(x,t)\,f(x)\,dx \tag{3.37}$$

Розглянемо числовий алгоритм з використанням *методу квадратур* для ІРФ І роду. Нехай перша частина $f(x)$ задана таблично на нерівномірній площині x, тобто на сітці вузлів $c = x_1 < x_2 < x_3 < \ldots < x_1 = d$.

Розв'язок $y_\alpha(s)$ шукається на іншій нерівномірній площині s, тобто на сітці вузлів, яка співпадає з площиною t, тобто сіткою вузлів $\alpha = s_1 = t_1 < s_2 = t_2 < s_3 = =< ... < s_n = t_n = b$, причому $t \neq n$.

Розпишемо інтеграл в (3.35) по довільно вибраній квадратурній формі, наприклад, по формулі трапецій. Отримаємо:

$$\alpha y_k + \sum_{i=1}^{n} r_j R_{ij} y_j = F_k;\ k = \overline{1,n}, \tag{3.38}$$

де $y_k = y_\alpha(t_k)$, $y_j = y_\alpha(s_j)$, $R_{kj} = R(t_k, s_j) F_k = F(t_k)$.

Аналогічно інтеграли в (3.36) та (3.37) апроксимуємо кінцевими сумами по квадратурной формулі. Отримаємо:

$$R_{kj} = R_{jk} = \sum_{i=1}^{l} p_i K_{ik} K_{ij}\ \text{, де } k, j = \overline{1,n};\ F_k = \sum_{i=1}^{l} p_i K_{ik} f_i\ \text{, де } k = \overline{1,n},$$

де $K_{ij} = K(x_i; t_k)$, $K_{jj} = K(x_i, s_j)$, $f_i = f(x_i)$, а r_j та p_i − коефіцієнти квадратурних формул.

Запис (3.38) є СЛАР відносно y_j, $j = \overline{1,n}$. В загальному випадку права частина $f(x)$ знаходиться на нерівномірной площині x, тобто на сітці вузлів $c = x_1 < x_2 < x_3 <::: < x_n = d$, а розв'язок $y(s)$ шукається на іншій нерівномірній площині s, тобто на сітці вузлів, яка співпадає з площиною t, тобто сіткою вузлів $\alpha = s_1 = t_1 < s_2 = t_2 < s_3 <::: < s_n = t_n = b$.

Викладене проілюструємо прикладом. З метою застосування регуляризації наведемо розв'язання некоректної лінійної задачі інтерпретації вимірювань або відновлення інформації. Як модельний сигнал використаємо квадратичну параболу, а як апріорну оцінку − лінійний профіль y_0, яким начебто можна описати невідомий сигнал, наприклад, такий, який представлено на рис. 3.5.

В результаті розв'язання СЛАР (останній рядку лістінгу програми в середовищі MathCAD; рис. 3.6), отримуємо залежність регуляризованого розв'язку вектора Y від F (рис. 3.7). Відповідна нев'язка системи рівнянь $\varepsilon(\alpha) = |AY(\alpha) - F|$, яка також є функцією x, приведена на рис. 3.8.

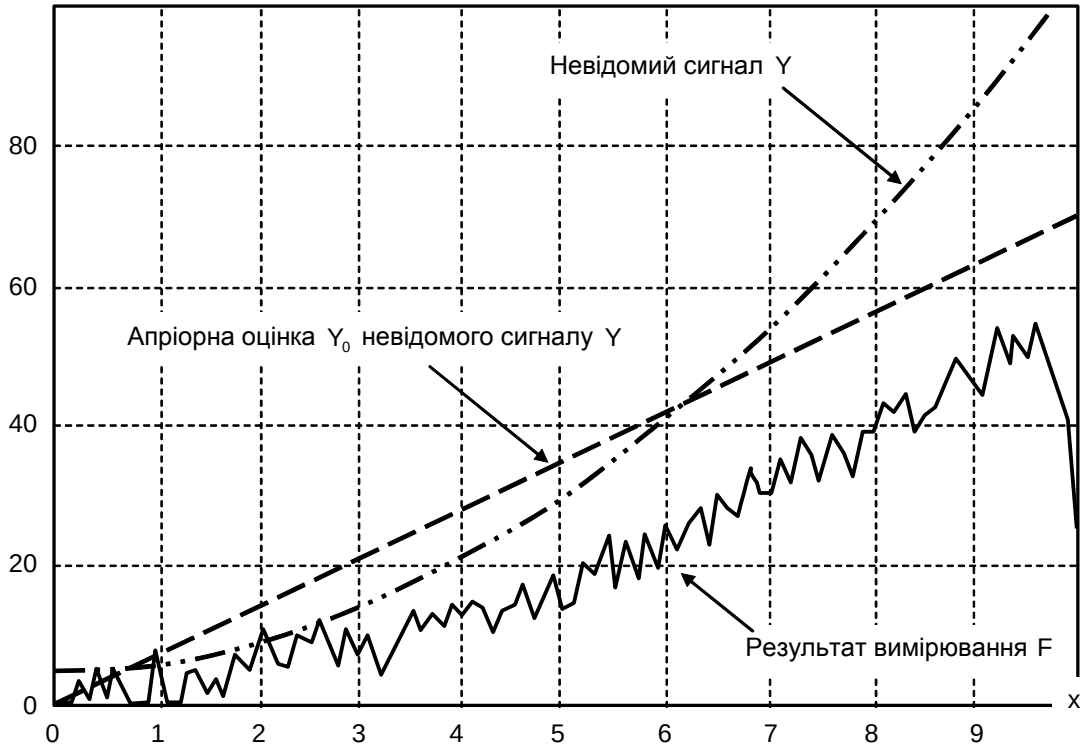
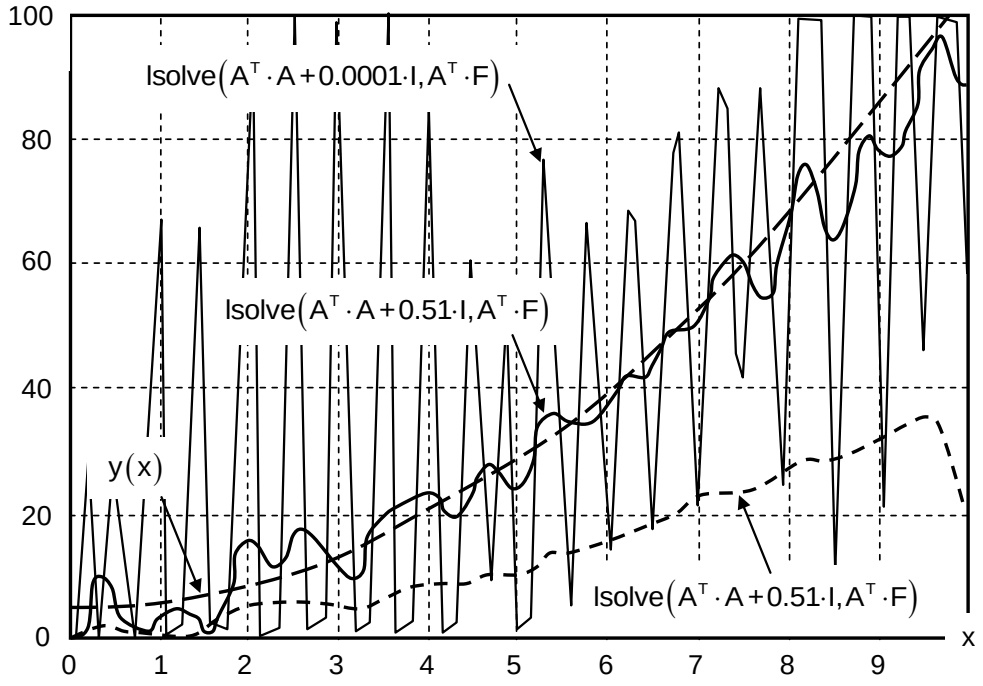


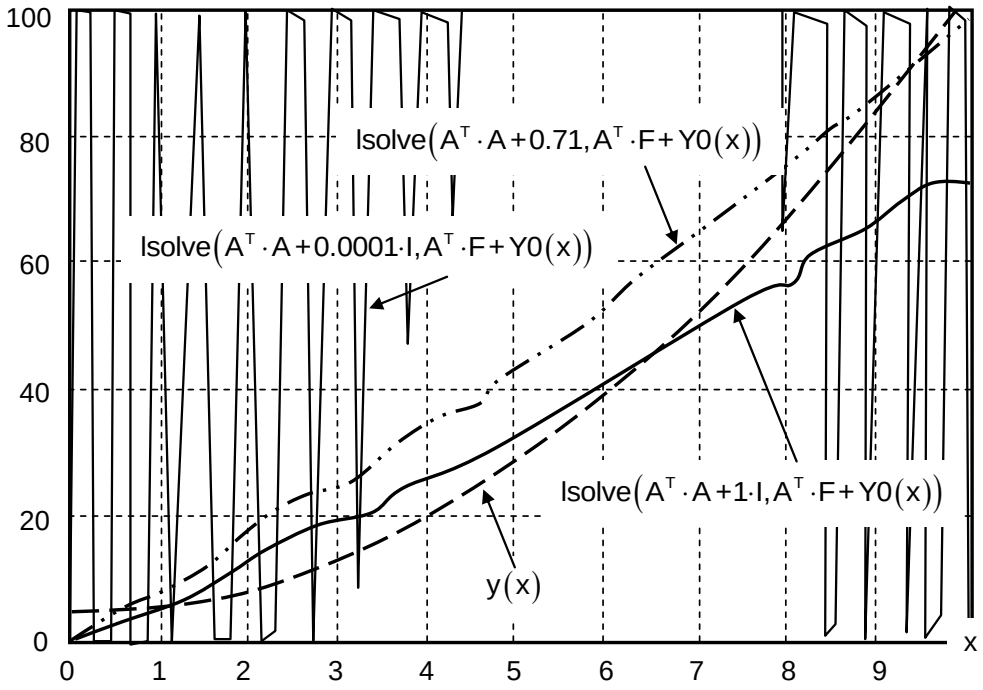
Рис. 3.5. Початковий (невідомий) сигнал Y та його апріорна оцінка Y_0 вимірювання F

$k := 10 \quad \sigma := 10$	Константи
$y(x) := 5 + x^2$	Модельний сигнал
$Y0(x) := 7 \times x$	Наближення модельного сигналу лінійним профілем
$A(x) := \exp(-k \times x^2)$	Ядро
$x := 0, 0{,}1 \ldots 10$	
	Додавання завади до виміряного сигналу:
$f(x) := \int_0^{10} A(\lvert x - s \rvert) \times y(s) ds + \sigma \times (rnd(1) - 0.5)$	
Дискретизація інтегрального рівняння квадратурами і застосування методу Тихонова. Параметр регуляризації А тут дорівнює 1, бо вибраний довільно	
$N := 10 \quad h := \frac{10}{N} \quad i := 0..N \quad j := 0..N \quad X_i := i \cdot h \quad A_{i,j} := A(\lvert X_i - X_j \rvert) \cdot h$	
$F_i := f(X_i) \quad \mu_{i,j} := \begin{cases} 1 \text{ if } i = j \\ 0 \text{ otherwise} \end{cases} \quad \alpha := 1 \quad Y(\alpha) := \text{lsolve}(A^T \cdot A + \alpha \cdot \mu A^T \cdot F + Y0(X))$	

Рис. 3.6. Листинг програми «Регуляризація некоректної лінійної задачі»

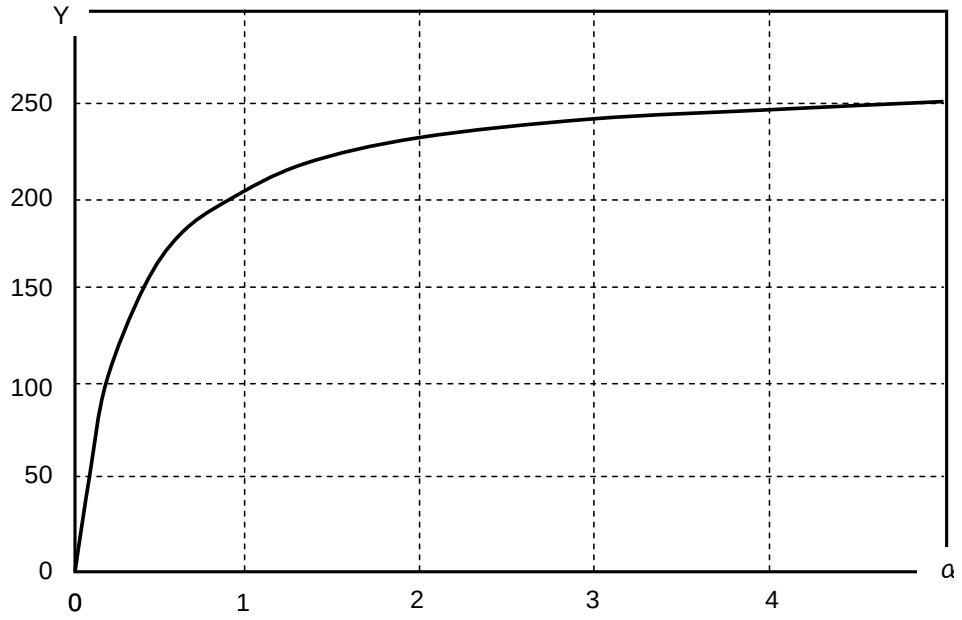


а)

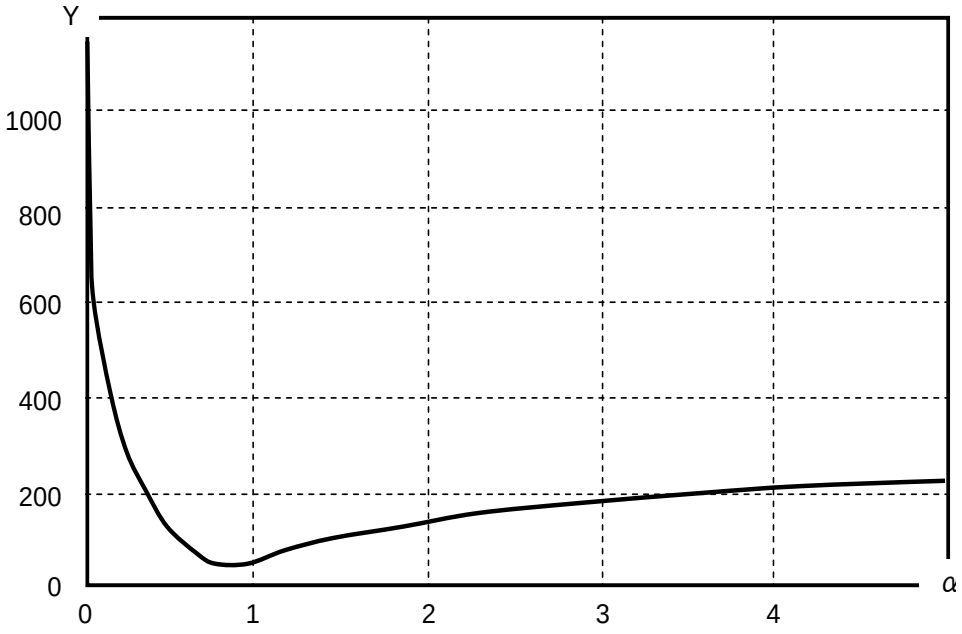


б)

Рис. 3.7 – Початковий (невідомий) сигнал та регуляризовані реконструкції при різних значеннях параметру регуляризації α при невідомій (а) та відомій (б) апріорній оцінці Y_0



а)



б)

Рис. 3.8. Нев’язка $\varepsilon(\alpha)$, отримана регуляризованим розв’язком $Y(\alpha)$ прикладу при невідомій (а) та відомій (б) апріорній оцінці Y_0

Т.ч., на основі застосування методу перетворення Фур'є, що оперує лише з векторами, розглянуте розв'язання інтегрального рівняння типу згортки – одномірного інтегрального рівняння Фредгольма I роду – в умовах існування некоректних задач. Отримане рішення розширює можливості рішення завдань, які можуть бути вирішені АСМІП стосовно використання пам'яті та часу розв'язання.

Для відновлення інформації при роботі АСМІП, слід враховувати, що можна використовувати таке значення α, яке відповідає глобальному мінімуму залежності $\varepsilon(\alpha)$. Інакше кажучи, АСМІП необхідно розв'язати ще одну задачу на знаходження мінімуму, але вже іншої функції $\varepsilon(\alpha)$. Підкреслимо, що саме визначення цієї функції передбачає вкладену мінімізацію функціоналу Тихонова, яка в поточному підрозділі представлена розв'язком системи лінійних рівнянь (3.30). Т.ч., для побудови реконструкції сигналу (див. рис. 3.7), тобто для відновлення інформації у критичних випадках, АСМІП доведеться вирішувати дві задачі мінімізації. Зазначимо, що знайти оптимальне α, як це зроблено в розглянутому прикладі, без використання Y_0 не вдалося (див. рис. 3.8). При $\varepsilon(\alpha) \to 0$ графік завжди нагадував «пилку» (рис. 3.7), яка була несхожою на невідомий сигнал, що свідчить про некоректність задачі.

3.5. Візуалізація структури показників якості функціонування інформаційно-вимірювальних систем галузі економіки, бізнесу та фінансів

Інформаційно-вимірювальні системи (ІВС) як загального використання, так і ті, що функціонують в галузі економіки, бізнесу та фінансів, описуються значним числом показників якості. При цьому показники, як правило, суперечливі. Задача оптимального вибору технічних параметрів, сигналів і структур, при яких досягається достатньо ефективне значення необхідних показ-

ників якості при заданих обмеженнях, є завданням оптимального синтезу зазначених параметрів, сигналів та структур. Саме постановка та розв'язок таких завдань для ескізного проектування ІВС представляє найбільшу складність. У цьому сенсі ще більшу складність представляє собою проектування систем оцінки якості функціонування ІВС (СОЯ ІВС) вище зазначеної галузі використання. Ще недавно це вважалося взагалі неможливим, якщо враховувати всі показники якості проектованої системи, які, як правило, встановлюються в технічному завданні (ТЗ). Як свідчать літературні джерела (огляд див. далі), прикладні задачі оптимального проектування систем оцінки якості функціонування ІВС мають специфічні особливості, до яких можна віднести багатоекстремальний та яружний характер функції якості, наявність обмежень на внутрішні та вихідні параметри ІВС та велику розмірність вектора варійованих параметрів.

Стратегія розв'язання задач оптимального проектування систем оцінки якості ІВС передбачає застосування глобальних процедур оптимізації на початкових етапах пошуку та уточнення отриманого глобального рішення локальними алгоритмами, які швидко сходяться та діють в околиці оптимальної точки. Така стратегія дозволяє з достатньою надійністю та точністю визначити значення глобального екстремуму та суттєво знизити обчислювальні витрати на пошук. При цьому етапи глобального пошуку можуть виконуватися з невисокою точністю, а етапи локального уточнення проводяться в області тяжіння глобального екстремуму, що вимагає значно меншого числа обчислень. Т.ч., з метою наочного представлення багатьох процесів оптимізації якості функціонування ІВС, задача візуалізації структури показників якості, яка винесена в заголовок підрозділу, є достатньо актуальною.

Аналіз останніх досліджень і публікацій показує, що стосовно проектування СОЯ ІВС є достатня кількість наукових робіт. Так, відомі наступні досягнення в області синтезу СОЯ ІВС та інших складних систем по сукупності показників якості [100-103] і т.д. У зазначених роботах викладені, з одного боку, досить загальні методи проектування та оптимізації СОЯ, з іншого –

приведені рішення окремих прикладних задач оптимізації по двом-трьом показникам якості, що не дозволяє з єдиних позицій та єдиним математичним апаратом виконати оптимізацію СОЯ ІВС по значному числу показників якості через недостатнє представлення їх структури. Інші відомі роботи з синтезу структури систем вимірювання як якісних показників, так і технічних параметрів взагалі, є досить частковими та скромними і занадто абстрактними. Це обмежує їх використання та не дає відповіді на питання про можливість загального оптимального синтезу СОЯ ІВС, про взаємозв'язки часткових видів їх синтезу, про єдину ідеологію оцінки якості вимірів та ін. [104]. Втім, у виробників, які виконують вимоги ТЗ, питання про оцінку показників якості та параметрів ІВС, виникати не повинно [105].

Зважаючи на сказане, метою підрозділу є розгляд та візуалізація структури показників якості ІВС з ціллю їх ранжування та врахування при проектуванні СОЯ.

Особливістю побудови сучасних ІВС галузі економіки, бізнесу та фінансів є використання топологічної структури типу «ієрархічна зірка», як показано на рис. 3.9. Саме така структура буде основою для подальших досліджень [106].

На нижньому рівні «зірки» знаходяться інтелектуальні датчики (ІД), які повинні забезпечити безпосереднє сприйняття від об'єкту вимірювання та перетворення характеристик досліджуваних подій і/або величин в уніфіковані сигнали. Т.ч., на рис. 3.9 інтелектуальні датчики позначені, як $ІД_{ik}$, де i – номер базуючого пристрою, $i = 1,...,N$; k – номер датчика, $k = 1,...,n$.

Наступний рівень ієрархії – центральний обчислювач (ЦО). На рис. 3.9 такі пристрої позначені як $ЦО_i$. ЦО обслуговують групи інтелектуальних датчиків. Основне завдання $ЦО_i$ – обмін даними з $ІД_{ik}$, управління їх роботою, корекція, розрахунок та кодування отримуваної вимірювальної інформації, а також обмін даними з вищестоящим ієрархічним рівнем. В даному прикладі верхнім рівнем ієрархії є електронно-обчислювальна машина (ЕОМ), завданням якої є обробка, відповідно до закладених алгоритмів, вимірювальної ін-

формації, що поступає, і обмін даними з іншими системами. Обмін даними між рівнями здійснюється по каналах зв'язку.

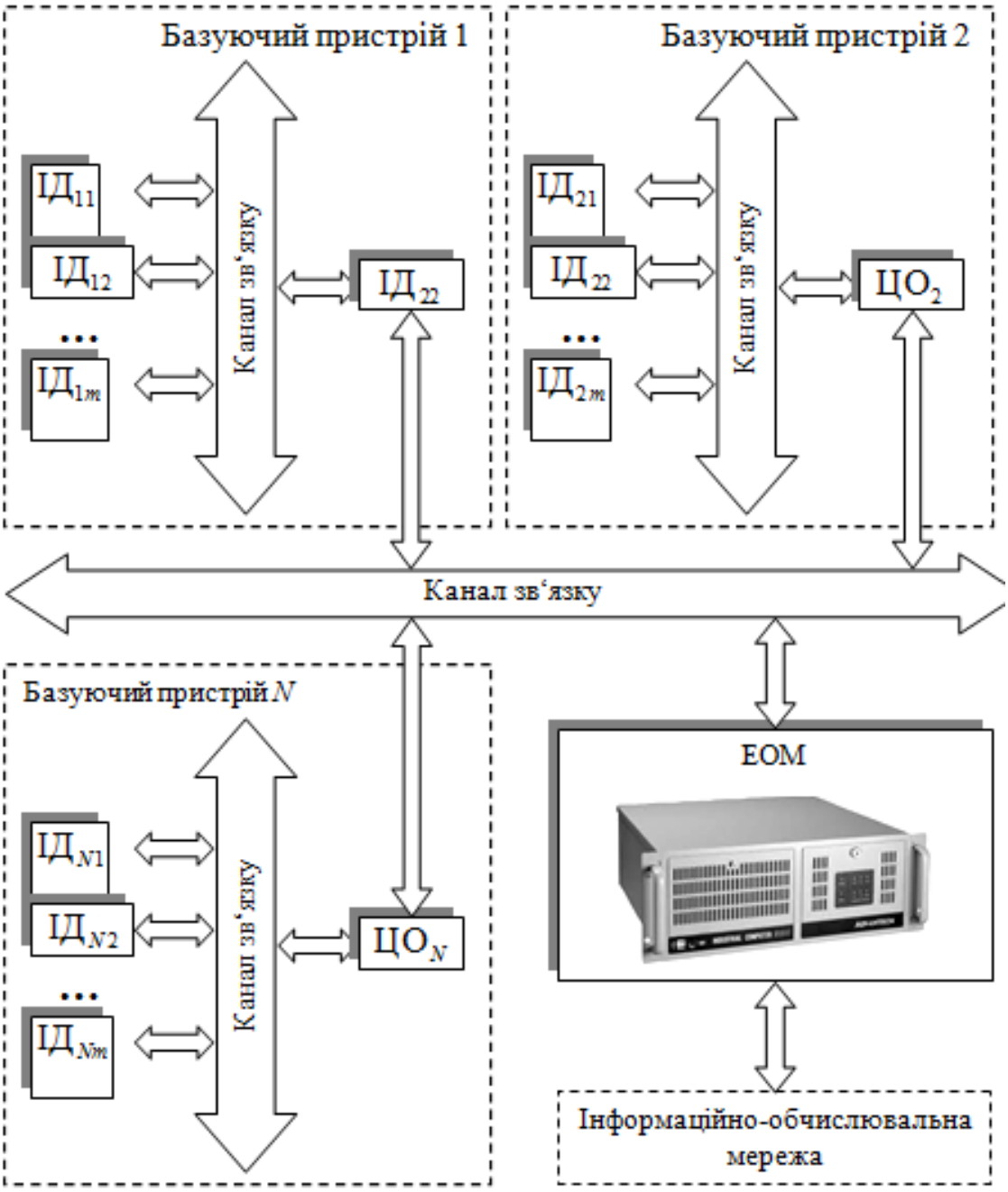


Рис. 3.9. Структура сучасних ІВС,
використовуваних у галузі економіки, бізнесу та фінансів

Як видно з рис. 3.9, кожен з рівнів вирішує свою задачу та є деякою сукупністю апаратних та програмних засобів: по термінології ГОСТ 22315-77 – сукупність агрегатних засобів.

Узагальнимо структурну схему трирівневої ІВС, яка зображена на рис. 3.9, та представимо її у вигляді графа (рис. 3.10).

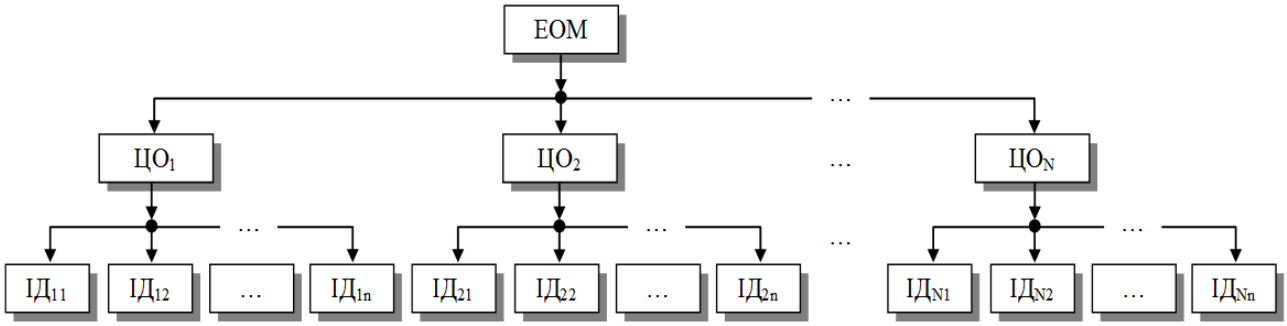


Рис. 3.10. Граф структурної схеми узагальненої ІВС

На рис. 3.10 агрегатні засоби показані у вигляді вершин графа, а його ребрами є канали передачі даних, які пов'язують різні ієрархічні рівні між собою. Вузол графа, не залежно від рівня, представляє деяку обчислювальну систему. У ній, як показано в [107], існують три основні складові, які впливають на якість функціонування ІВС: *технічні засоби; програмне забезпечення; інформаційне забезпечення.* Показники якості кожної зі складових встановлюються на основі відповідних стандартів. Крім складових, які наведені на рис. 3.10, при проектуванні систем оцінки якості ІВС, також слід брати до уваги економічну компоненту, яка визначає проектну, виробничу, експлуатаційну та загальну вартість системи.

Спочатку, з метою спрощення задачі, розглянемо алгоритм формування структури узагальненого показника якості функціонування ІВС. Як випливає з рис. 3.10, представлений граф являє собою сукупність автономних вузлів (ізольованих систем), кожен з яких, не залежно від рівня ієрархії, володіє своїми показниками якості. Як уже зазначалося, показники визначені у технічному завданні. Узагальнену структуру дерева властивостей вузла покажемо у вигляді рис. 3.11.

Визначення показників якості автономних систем, включаючи ІВС, зручно проводити на стадії проектування: саме на цій стадії проводиться аналіз

вимог технічного завдання, визначається склад системи в цілому, вибираються характеристики окремих технічних засобів, розробляються алгоритми програмного та інформаційного забезпечення. Питання полягає в тому, що при зовнішній своєї незалежності складові забезпечення функціонування вузла тісно пов’язані між собою. Так, наприклад, неякісний алгоритм і програмний код можна компенсувати поліпшенням технічних характеристик так, як це показано на рис. 3.12, а недоліки технічної та програмної складової – оптимізацією інформаційних потоків – рис. 3.13.

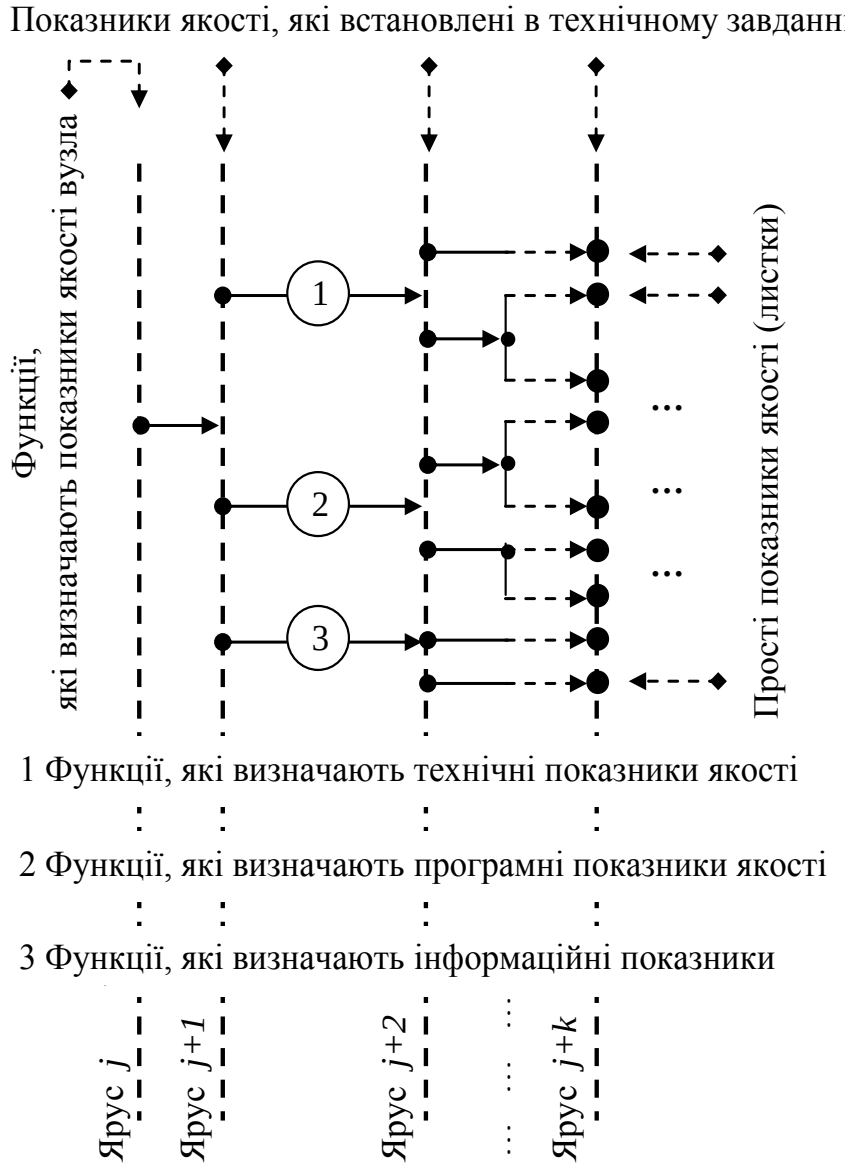


Рис. 3.11. Візуалізація узагальненої структури дерева властивостей вузла у вигляді графу

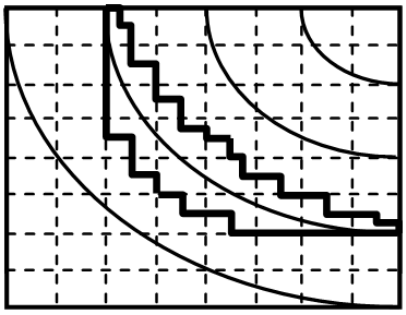


Рис. 3.12. Пояснення до технології компенсації неякісного алгоритму або програмного коду поліпшенням технічних характеристик

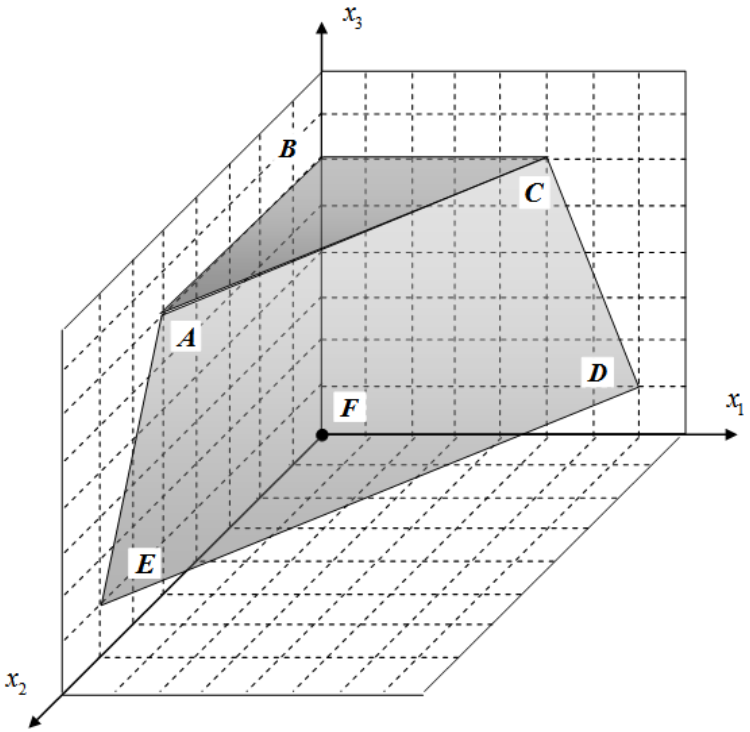


Рис. 3.13. Пояснення до технології компенсації технічної та програмної складової

Найбільший інтерес представляє визначення якості функціонування системи в цілому – функціональний рівень узагальнених показників якості (УПЯ). Як видно з графа (рис. 3.10), тут необхідно враховувати як вплив якісних складових окремих вузлів на функціонування їх сусідів (по ієрархічному рівню), так і вплив вище стоячих або нижче стоячих вузлів.

Синтезована конструкція являє собою багатовимірну структуру, яку графічно представимо у вигляді комірчастого тривимірного об’єкту (рис. 3.14).

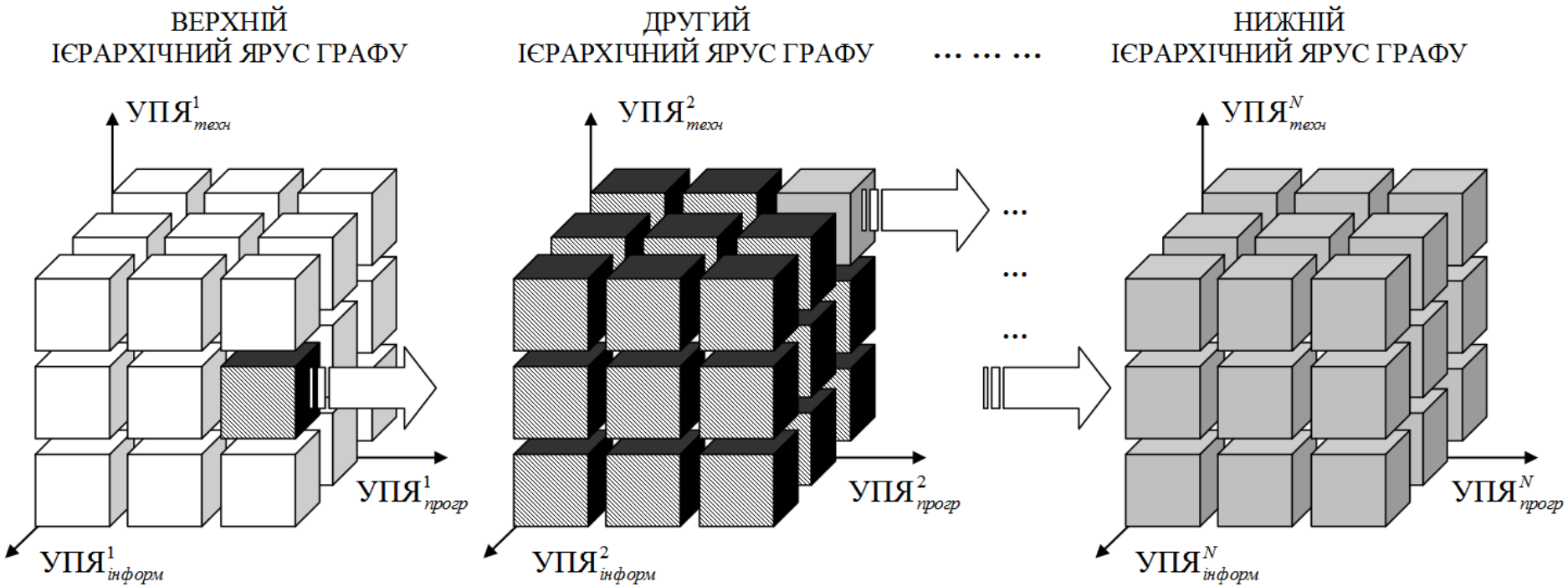


Рис. 3.14. Візуалізація синтезу структури функціонального рівня УПЯ у вигляді багатовимірного об’єкту

За принципом вкладеності об’єктів один в одного, кожному вузлу графа призначається осередок з вкладеним в нього осередком вузла більш низької ієрархії. Осями кожного осередку та об’єкта в цілому, є значення УПЯ технічних засобів, програмного та інформаційного забезпечення. З рис. 3.14 видно, що кожен УПЯ формується з показників, які встановлені раніше для відповідного вузла і вказані в ТЗ – див. рис. 3.11.

Розгортання багатовимірного об’єкта в плоску фігуру дає узагальнене дерево властивостей функціональної корисності ІВС. Покажемо це у вигляді рис. 3.15. На ньому звернемо увагу на розміщення якісних показників на відповідних ярусах дерева незалежно від ієрархічного рівня вузла графа.

Згідно до діючих стандартів, УПЯ продукції, крім функціональних показників, включають і такі показники, як естетичний, транспортабельності, патентно-правовий та ін. Введення цих показників веде ще до більшої розмірності багатовимірності дерева властивостей (див. рис. 3.16).

Економічні показники якості, що представляють вартість системи на етапах життєвого циклу, в загальному випадку, також є багатомірним об’єктом. Побудова дерева властивостей економічного УПЯ здійснюється аналогічно розглянутому вище УПЯ продукції та знаходиться з ним на одному ярусі дерева властивостей (рис. 3.17).

Інтегральний показник якості ІВС, відповідно до визначення, включає УПЯ економічної складової. Кінцеве його значення можна виразити двовимірним вектором, де, відповідно до правила Парето, по осі ординат відкладено оптимізований вектор економічного УПЯ, а по осі абсцис – оптимізований УПЯ продукції (рис. 3.18).

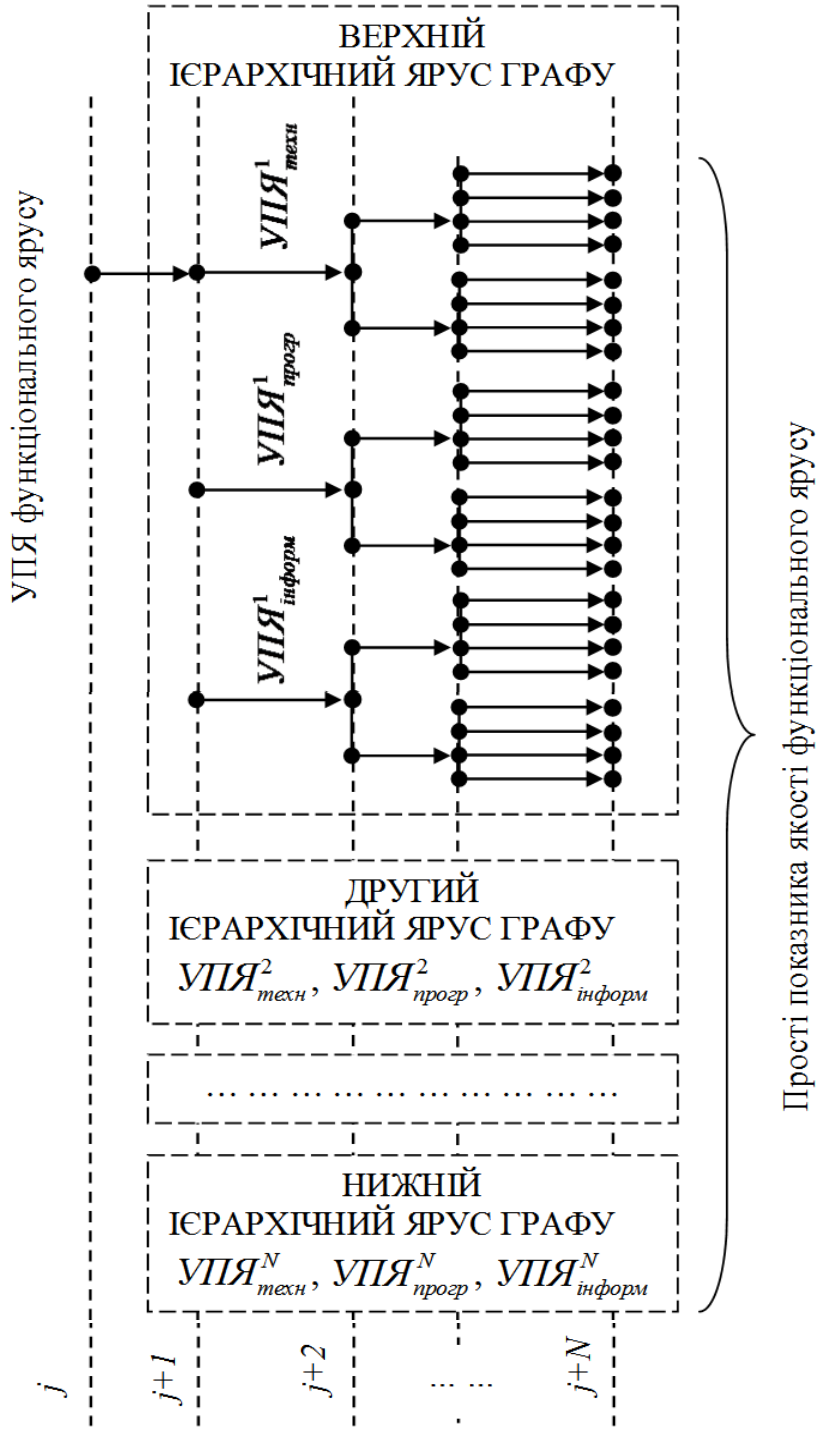


Рис. 3.15. Візуалізація узагальненого дерева властивостей функціональної корисності ІВС у вигляді плоскої фігури

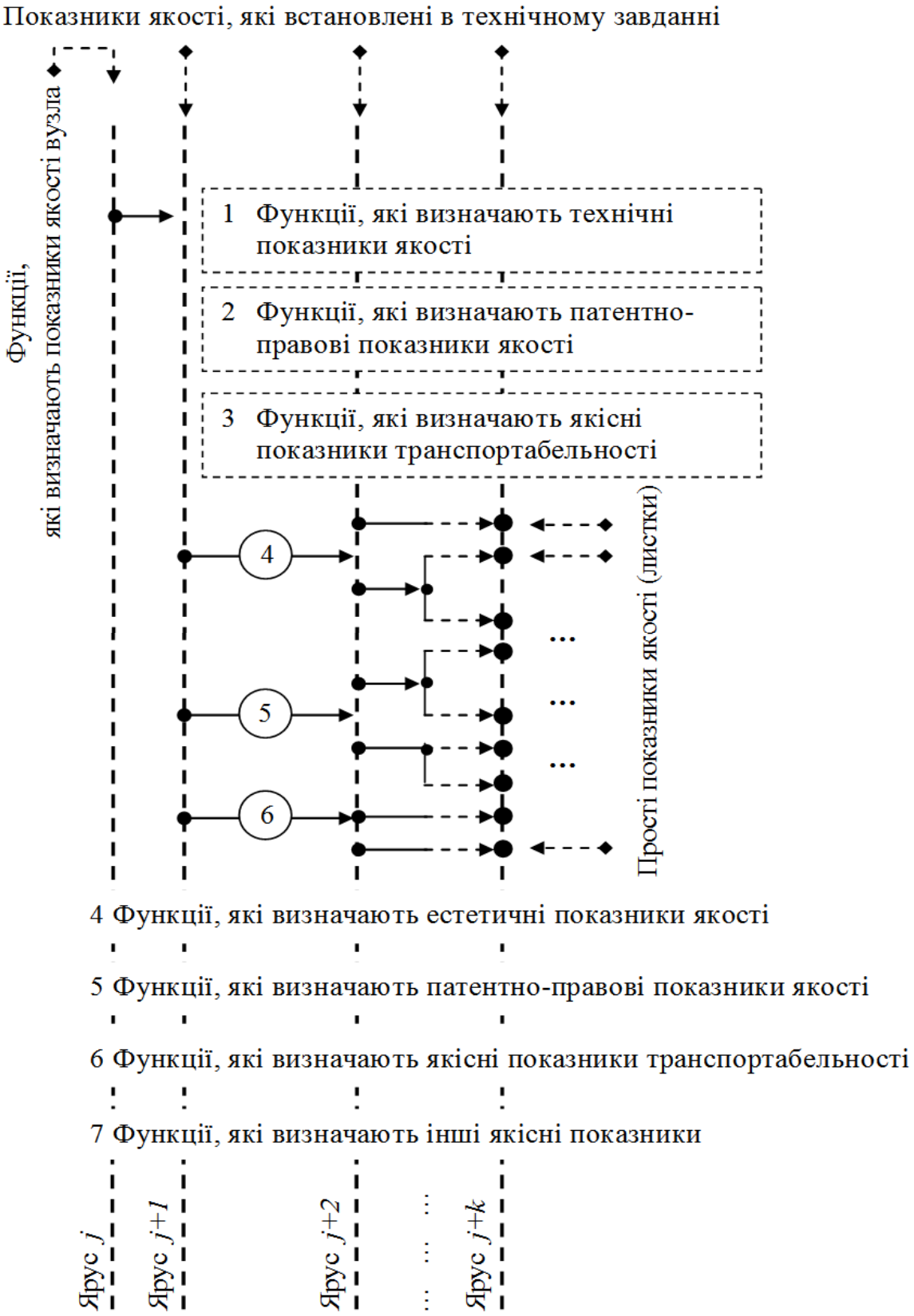


Рис. 3.16. Візуалізація збільшення багатовимірності дерева властивостей

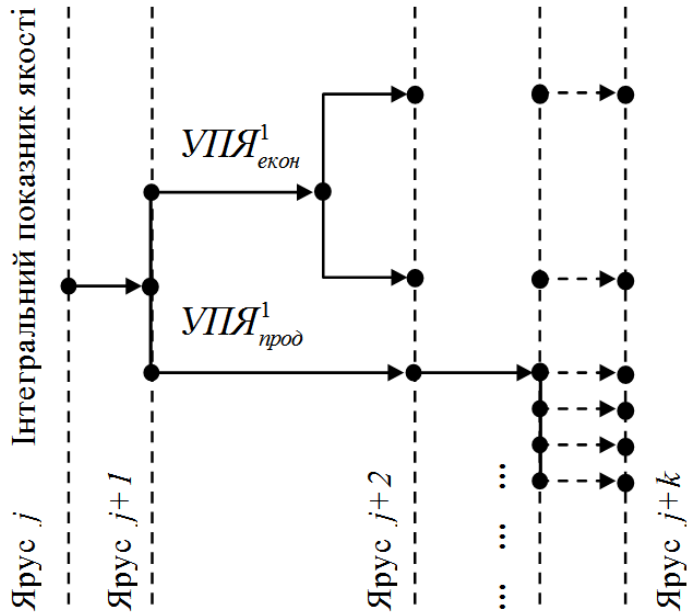


Рис. 3.17. Візуалізація дерева властивостей з урахуванням економічного УПЯ

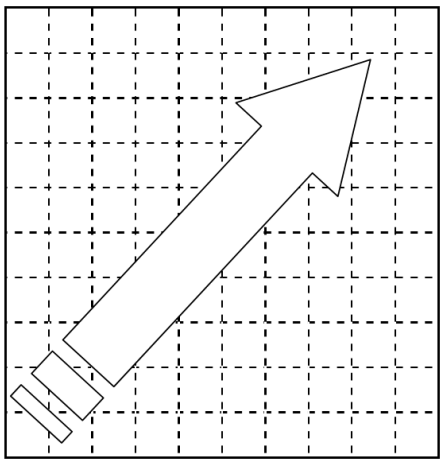


Рис. 3.18. Візуалізація інтегрального показника якості ІВС

Приведені результати візуалізації структури показників якості з метою їх ранжування та врахування при проектуванні СОЯ ІВС, що надає можливості розробки стратегії розв’язання задач оптимального проектування таких систем при застосуванні глобальних процедур оптимізації на початкових етапах пошуку та при уточненні отриманого глобального рішення локальними алгоритмами.

3.6. Принципові питання вирішення задачі багатокритеріальної оптимізації показників якості інформаційно-вимірювальних систем галузі економіки, бізнесу та фінансів на основі мультихромосомного генетичного алгоритму

При сучасному розвитку інформаційних технологій визначальне значення для практики підтримки прийняття рішень набувають методи оцінки станів об’єктів. Як правило, при оцінці якості технічних систем до яких відносяться інформаційно-вимірювальні системи (ІВС) галузі економіки, бізнесу та фінансів, на кожному з етапів їх життєвого циклу виділяються істотні фактори, що спричиняють найбільший вплив на цільову функцію управління, і з урахуванням цих факторів або груп параметрів проводиться оцінка ефективності функціонування об’єкта [108]. На основі прийнятих рішень далі може йти мова про оптимізацію показників якості технічної системи.

Аналіз останніх досліджень і публікацій показує, що в основі оптимізації технічних систем лежить системний аналіз (СА). Його означення та процедура проведення є, наприклад, у [109]. Результатом СА є вибір з множини можливих варіантів побудови системи на підставі аналізу та перебору, одного варіанту, який буде вважатися оптимальним, тобто задовольняти деякому критерію (критеріям). При аналізі складних систем задача оптимізації розглядається як багатокритеріальна, а її результат – як один з кращих варіантів, що погоджує ряд суперечливих вимог до рішення, яке приймається.

Одним з напрямків СА є вивчення процесів проектування, створення, випробування та експлуатації складних технічних систем з орієнтацією цих процесів на досягнення максимального підвищення якості. У нашому випадку – на побудову оптимальних за співвідношенням показників якості технічних засобів, програмного та інформаційного забезпечення ІВС. Згідно до загальновідомих означень, якість, як сукупність характеристик об’єкта (системи), що відносяться до його здатності задовольняти встановлені або передбачувані потреби, представляє собою багатовимірний об’єкт, для дослідження якого можуть бути корисні підходи та результати, отримані в результаті сис-

темного аналізу.

Галуззю науки, яка вивчає та реалізує методи кількісної оцінки якості об’єктів реального світу, є кваліметрія. Кваліметрія є частиною квалітології – науки про якість. Базуючись на цьому, в основу дослідження, на відміну від відомих методів дослідження ІВС з використанням генетичних алгоритмів (ГА), які мають у своєму підґрунті синергетичні методи, нами покладений саме кваліметричний підхід: в кваліметрії, при аналізі, синтезі та пошуку оптимуму якості об’єктів, можуть застосовуватися методи системного аналізу і навпаки, системний аналіз включає в себе кваліметричну оцінку показників системи.

Т.ч., процес оптимізації якості ІВС можна умовно розділити на п’ять взаємопов’язаних етапів:

1) побудова ієрархічної структури системи шляхом послідовного її розчленування на окремі підсистеми та елементи;

2) побудова графа (дерева) якості, який дає повну картину якісних і кількісних показників кожної складової та всієї системи в цілому;

3) розробка структурно-логічної схеми системи;

4) створення узагальненої моделі якості системи;

5) пошук оптимуму співвідношення показників якості системи.

Виходячи зі сказаного, формальною постановкою задачі підрозділу є виявлення факту того, чи повинна модель життєвого циклу кожної складової та системи в цілому визначатися в технічному завданні згідно до діючих стандартів. При цьому необхідно встановити, чи показники якості на кожному етапі життєвого циклу є комплексними показниками і чи ці показники складаються з відповідних показників технічних і програмних засобів та рішень.

На основі розгляду структури ІВС, яка застосовується в галузі економіки, бізнесу та фінансів, як програмно-апаратної системи, доцільним є формулювання вимог до складу генетичної моделі оцінки якості в цілому і видів забезпечення – зокрема на етапах життєвого циклу: проектуванні, виробництві, експлуатації. Виходячи з цього, необхідно піддати аналізу методи оптимізації

якості з урахуванням нечіткої інформації з метою обґрунтування необхідності розробки вдосконаленого методу, орієнтованого на генетичні алгоритми. З цієї точки зору виникає необхідність розгляду критеріїв оптимізації та формулювання пропозицій з комплексної оцінки якості ІВС з урахуванням видів забезпечення і етапів життєвого циклу, а також пропозицій щодо використання структури показників якості та керованих параметрів, які необхідно враховувати при розробці мультихромосомної генетичної моделі оцінки якості ІВС.

У неформальній формі завдання можна трактувати в такий спосіб: *потрібно знайти співвідношення параметрів елементів системи, які щонайкраще задовольняють заданим критеріям якості на всіх етапах життєвого циклу*.

Послідовне виконання пунктів процесу оптимізації приводить до побудови дерева властивостей (рис. 3.19).

Аналіз приведеного рисунка показує, що листи дерева будуть простими або квазіпростими показниками якості, які характеризують елементи системи; вузли – комплексні показники якості, які характеризують частини системи (підсистеми) та систему в цілому; а гілки визначають взаємозв'язки між показниками. У якості критеріїв, що визначають якість системи, можуть бути як комплексні показники якості (КПЯ), так і прості або квазіпрості показники (ППЯ). При цьому тут розуміється, що такі показники характеризують лише співвідношення програмно-технічних компонентів системи без урахування економічної складової.

На підставі дерева властивостей з'являється можливість побудови математичної моделі критеріїв якості системи. Виходячи з позначень, наведених на рис. 3.19, представимо узагальнений код ППЯ в наступному вигляді: $Z_k Y_k X_k ... B_k A_k A_0$, де $A, B, ... Z$ – яруси дерева властивостей; k – номер вузла (показника якості) в ярусі $(k = 1, 2, ..., m)$; A_0 – інтегральний показник якості.

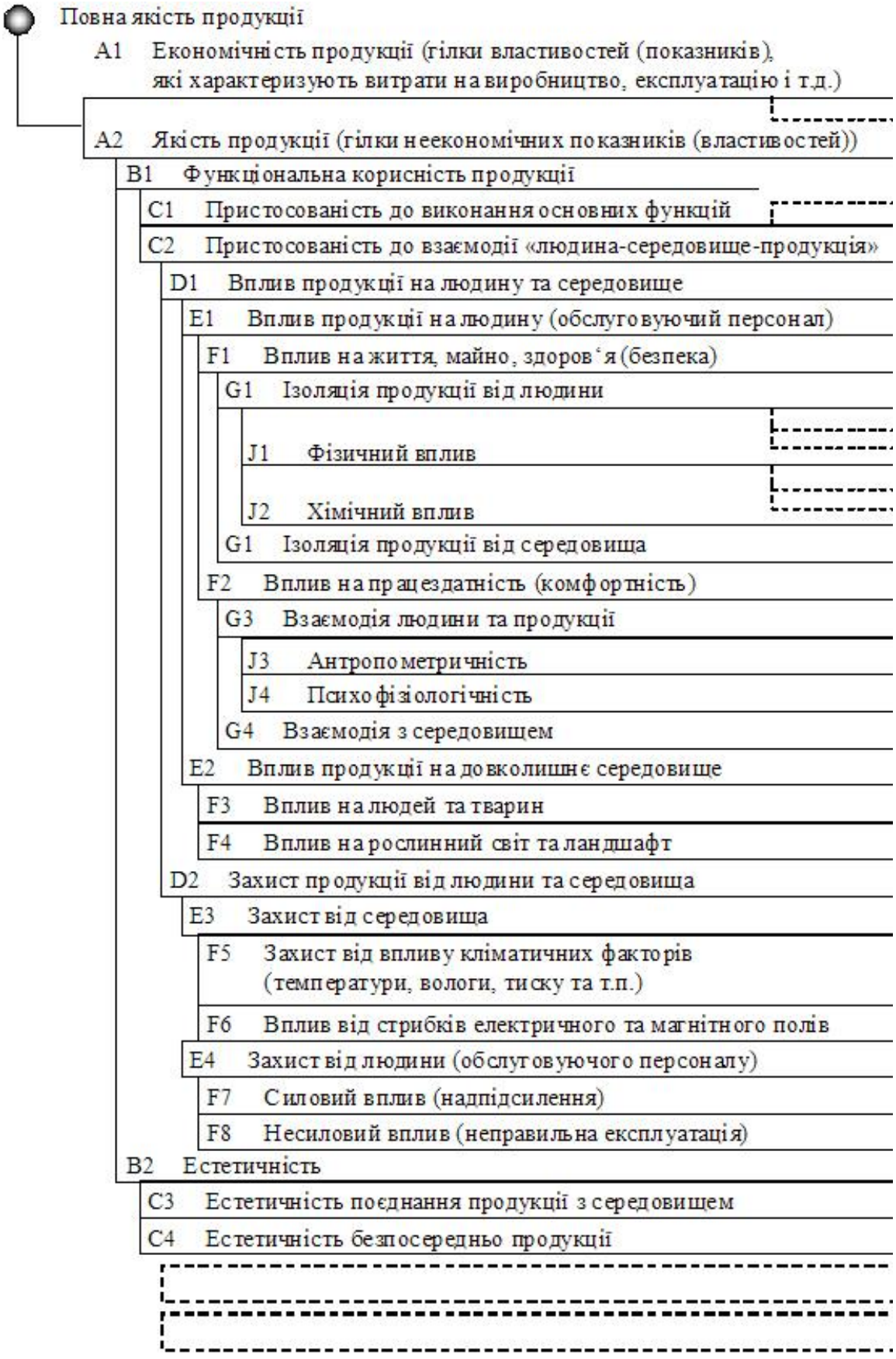


Рис. 3.19. Узагальнене дерево властивостей деякої умовної системи

З метою формування цільової функції (ЦФ), розглянемо рис. 3.20.

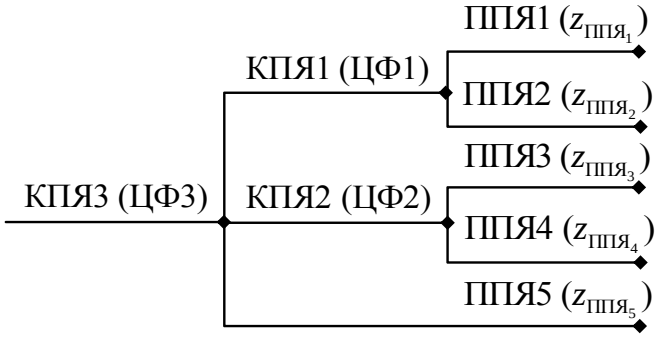


Рис. 3.20. Фрагмент ярусів дерева властивостей

Слідуючи з приведеного рисунка та з врахуванням того, що $K_i = \left\{ L_i \cup K_{i+1}^{k_{i+1}} \right\}$, де K_i – множина показників властивостей *i*-го ярусу $(i = 1,2,3,...)$, K_{i+1} – множина показників властивостей *i*+1-го ярусу, k_{i+1} – міpність множини *i*+1-го ярусу $\left(k \in \square^{+}\right)$, L_i – множина ППЯ *i*-го ярусу $\left(L_i \subset K_i\right)$, будь-який КПЯ можна представити як суму множин ППЯ поточного ярусу та множин КПЯ наступного ярусу дерева властивостей. Як видно, значення показників будуть векторною оцінкою можливого рішення $f(x) = (f(x_1), f(x_2),..., f(x_n))$, таким чином:

$$\text{ЦФ}_1 = f\left(z_{ППЯ_1}, z_{ППЯ_2}\right);$$
$$\text{ЦФ}_2 = f\left(z_{ППЯ_3}, z_{ППЯ_4}\right);$$
$$\text{ЦФ}_3 = f\left(\text{ЦФ}_1, \text{ЦФ}_2, z_{ППЯ_5}\right) = f\left(z_{ППЯ_1}, z_{ППЯ_2}, z_{ППЯ_3}, z_{ППЯ_4}, z_{ППЯ_5}\right),$$

де $\text{ЦФ}_1, \text{ЦФ}_2, \text{ЦФ}_3$ − цільові функції, які відповідно визначають значення КПЯ_1, КПЯ_2, КПЯ_3; $(z_{ППЯ_1},..., z_{ППЯ_5})$ − значення ППЯ_1, ППЯ_2, ППЯ_3, ППЯ_4 та ППЯ_5 відповідно.

Узагальнюючи наведені вище вирази на дерево властивостей, запишемо:

$$\begin{aligned} \text{ЦФ}_{rj} = f\left(\text{ЦФ}_{1\,j+1}, \text{ЦФ}_{2\,j+1},..., \text{ЦФ}_{ij+1},..., \text{ЦФ}_{nj+1}, z_{ППЯ_{1rj}}, z_{ППЯ_{2rj}},..., z_{ППЯ_{arj}},..., z_{ППЯ_{mrj}}\right) = \\ = f\left(z_{ППЯ_{1rj}}, z_{ППЯ_{2rj}},..., z_{ППЯ_{brj}},..., z_{ППЯ_{vrj}}\right), \end{aligned} \quad (3.39)$$

де: $ЦФ_{rj}$ − цільова функція КПЯ відповідного вузла r ярусу j дерева властивостей $(j = 0,1,2,...,k-1)$; $ЦФ_{ij+1}$ − цільова функція КПЯ вузла i $(i = 1,2,...,n)$ ярусу $j+1$ дерева властивостей (параметр функції $ЦФ_{rj}$); $z_{ППЯ_{arj}}$ − значення, що $ППЯ_{arj}$ є параметром функції $ЦФ_{rj}$ $(a = 1,2,...,m)$; $z_{ППЯ_{brj}}$ − значення, що $ППЯ_{brj}$ є параметром функції $ЦФ_{rj}$ або функції $ЦФ_{ij+1}$; $(b = 1,2,..., v)$.

Т.ч., як видно, у процесі моделювання, шляхом послідовного проходу по листах, гілках та ярусах дерева властивостей, на основі узагальнення коду ППЯ у вигляді $Z_k Y_k X_k ... B_k A_k A_0$, для кожного з обраних критеріїв по формулі (3.39) можемо синтезувати вирази для визначення ЦФ. Далі можемо синтезувати особини з використанням мультихромосомного генетичного алгоритму.

Наступна фаза роботи ГА – це формування популяції та циклічне, до виникнення заданої умови виходу із циклу, виконання стандартних ГО по відомих методиках, які достатньо докладно викладені у численній науковій літературі.

Розрахунки значень ЦФ критеріїв є однією з найбільш важливих задач, розв'язуваних у процесі оптимізації системи. Розглянемо фрагмент дерева властивостей, представлений на рис. 3.21.

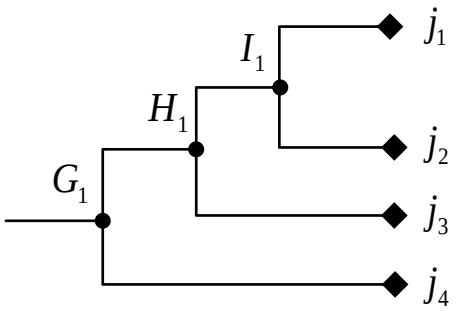


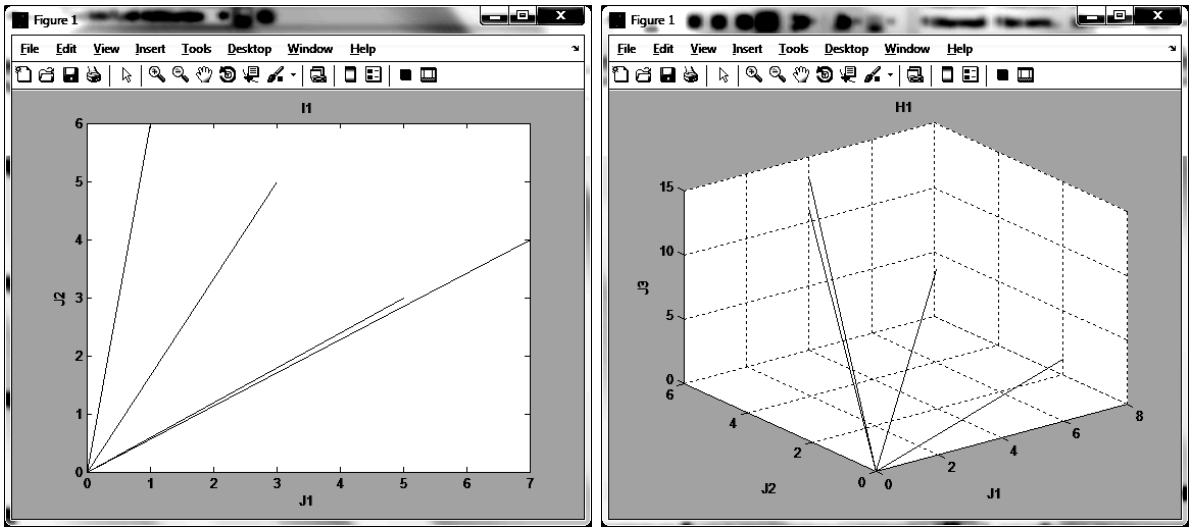
Рис. 3.21. Фрагмент дерева властивостей

Нехай критеріями якості будуть вузли I_1, H_1, G_1 та ППЯ J_3 і J_4. Тоді, відповідно до вище наведеної методики формування ЦФ, можемо записати:

$I_1 = f(J_1, J_2)$; $H_1 = f(I_1, J_3) = f(J_1, J_2, J_3)$; $G_1 = f(H_1, J_4) = f(I_1, J_3, J_4) = f(J_1, J_2, J_3, J_4)$,

де ППЯ J_1, J_2, J_3, J_4 будуть параметрами векторних оцінок.

Вигляд векторних оцінок, які розраховані для критеріїв I_1 та H_1, приведений на рис. 3.22,а та б – відповідно.



а) б)

Рис. 3.22. Вигляд векторних оцінок, які розраховані для критеріїв I_1 (а) та H_1 (б)

Визначення функцій приналежності деякої величини нечіткій множини в багатомірних областях визначення, що є декартовим добутком X деякого числа n складових їхніх областей $(X_1,...,X_n)$, дане в [110]. Відповідно до теорії нечітких множин, синтезуємо означення для випадку функції бажаності Харрінгтона d, тобто покажемо приналежність векторної оцінки показника якості метричній шкалі Харрінгтона.

Означення 1. Класичним n-арним відношенням R, яке задане на області визначення $Z_{ІПЯ} = Z_1 \times Z_2 \times ... \times Z_n$, називатимемо впорядковану множину кортежів з n елементів, тобто:

$$R = \left\{ \left((z_1,...,z_n), \mu_R(z_1,...,z_n) = d \right) \middle| (z_1,...,z_n) \in Z_{ІПЯ} \right\},$$

де: *ІПЯ* – інтегральний показник якості, який характеризує співвідношення економічної та технічної компонент системи; Z_i – можливі значення i-го

ППЯ; $(z_1,...,z_n)$ – кортеж, ступінь приналежності якого відношенню R дорівнює $\mu_R(z_1,...,z_n)$; $d=\mu_R(z_1,...,z_n)=1,$ якщо$(z_1,...,z_n)\in R;$ $d=\mu_R(z_1,...,z_n)=0,$ якщо$(z_1,...,z_n)\notin R.$

Функція приналежності класичного відношення відображає область визначення $Z_{ІПЯ}$ на дискретну множину $\{0,1\}$, тобто $d=\mu_R: Z_1\times...\times Z_n\to\{0,1\}$.

Означення 2. Нечітким n-арним відношенням R, яке задане на області визначення $Z_{ІПЯ}=Z_1\times Z_2\times...\times Z_n$, називатимемо впорядковану множина кортежів з n елементів, тобто:

$$R=\left\{\left((z_1,...,z_n),\mu_R(z_1,...,z_n)=d\right)\middle|(z_1,...,z_n)\in Z_{ІПЯ}\right\}, \qquad (3.40)$$

де: Z_i – можливі значення i-го ППЯ; $(z_1,...,z_n)$ – кортеж, ступінь приналежності якого відношенню R дорівнює $\mu_R(z_1,...,z_n)$.

Функція приналежності нечіткого відношення відображає область визначення $Z_{ІПЯ}$ на безперервний інтервал $[0,1]$:

$$d=\mu_R(z_1,...,z_n): Z_1\times...\times Z_n\to[0,1].$$

У загальному випадку функція бажаності Харрінгтона d відношення R являє собою гіперповерхню в $(n+1)$ мірному просторі, де n – кількість ППЯ і/або квазіпростих показників якості формуючого критерію на підставі дерева властивостей (див. рисунки).

Для критеріїв, які мають фізичний смисл (ФК), розрахунок значення ЦФ може бути проведений з використанням аналітичного виразу, який визначає сам ФК. При цьому його параметрами будуть $z_{ППЯ_i}^{ФКj}$ відповідного етапу життєвого циклу ІВС.

Складемо алгоритм розрахунків значення ЦФ і функції Харрінгтона для ФК:

Крок 1. Вибірка з хромосоми двійкового коду гена, який відповідний i-му ППЯ j-го ФК.

Крок 2. Зворотне перетворення довжин кодових послідовностей генів.

Крок 3. Переклад із заданою точністю двійкового коду гена в десяткове

значення. Отримане число буде відповідати значенню ППЯ, кодованому відповідно до додаткової метричної шкали, яка може бути введена за особливими (необхідними) встановленими критеріями.

Крок 4. Переклад кодованого значення ППЯ з додаткової метричної шкали в код шкали Харрінгтона шляхом зсуву отриманого десяткового значення на величину $z'_{\min}$ вліво.

Крок 5. Зворотне перетворення значення ППЯ кодованого у відповідності зі шкалою Харрінгтона зі значення z'_i в z_i, тобто одержання поточного фізичного значення параметра $z_{ППЯ_i}^{ФКj}$.

Крок 6. Розрахунки значення ФК (довжини вектора – див. рис. 3.22) з використанням відповідного аналітичного виразу

$$f_{ФК_j} = f\left(z_{ППЯ_1}^{ФКj},...,z_{ППЯ_i}^{ФКj},...,z_{ППЯ_n}^{ФКj}\right),$$

де n − кількість параметрів (ППЯ), які відносяться до даного критерію.

Крок 7. Розрахунок функції бажаності Харрінгтона d для отриманого значення ФК. Залежно від постановки завдання (визначення припустимих значень ФК – довжин векторів) можливі два варіанти розв'язку.

Варіант 1. Задане чітке обмеження у вигляді лінгвістичного значення з чіткими границями, наприклад: значення ЦФ критерію I_1 (рис. 3.21) $ЦФ_{I_1} = f\left(J_1, J_2\right)$ не повинне перевищувати $z_{\max}$ $(z_{I_1} \le z_{\max})$. У цьому випадку при визначенні d_{I_1} будемо використовувати бінарне відношення $R = \left\{\left(z_{I_1}, z_{I_2}\right), \mu_R\left(z_{I_1}, z_{I_2}\right) = d_{I_1}\right\}$, де $d_{I_1} = \{0,1\}$.

Представлення d_{I_1} у вигляді дискретної тривимірної функції приналежності, змодельоване в LabVIEW, приведене на (рис. 3.23).

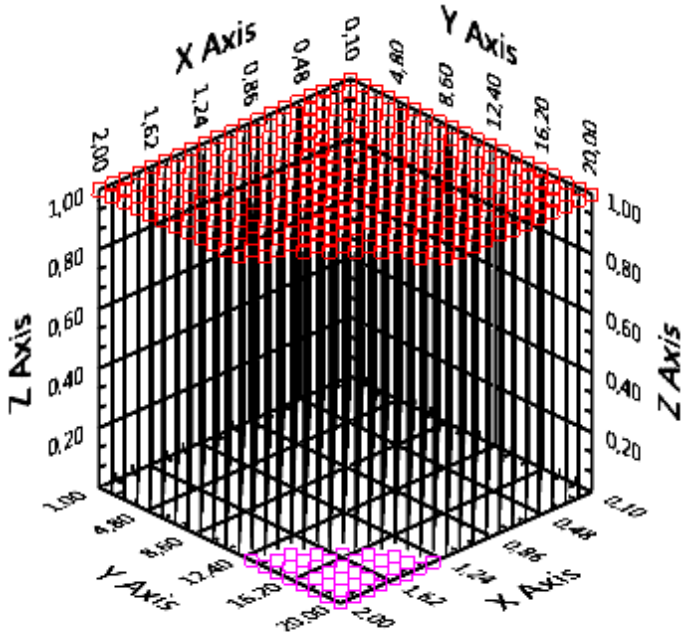


Рис. 3.23. Розраховане представлення d_{I_1} у вигляді дискретної тривимірної функції приналежності, де вісь Z відповідає функції бажаності Харрінгтона d ФК I_1; вісь X – значенням параметра J_1; вісь Y – значенням параметра J_2

Варіант 2. Задане нечітке обмеження у вигляді лінгвістичного значення з нечіткими границями. У цьому випадку при визначенні d використовуватимемо нечітке відношення, а замість дискретної множини $d=\{0,1\}$ розглядатимемо безперервний інтервал $d=[0,1]$. Наприклад: значення ЦФ критерію I_1 (рис. 3.21) $ЦФ_{I_1}=f\left(J_1,J_2\right)$ повинне бути мінімальним і не повинне перевищувати $z_{\max}$. При визначенні d_{I_1} використовуватимемо нечітке відношення (3.40). Представлення d_{I_1} у вигляді безперервної тривимірної функції приналежності, змодельоване в LabVIEW, приведене на (рис. 3.24).

Як видно, обидва варіанти розв'язку дають значення довжини вектора d, який розташований на $(n+1)$ осі просторових координат ФК.

Складемо алгоритм для ЦФ критеріїв, які мають логічний смисл (ЛК). Аналітичний вираз подібний до виразу для розрахунків ЦФ ФК, у випадку ЛК відсутній, хоча його векторна оцінка може бути побудована за значеннями простих і квазіпростих ПЯ, як це показано на рис. 3.21. Тому метою алгоритму є визначення значення функції Харрінгтона.

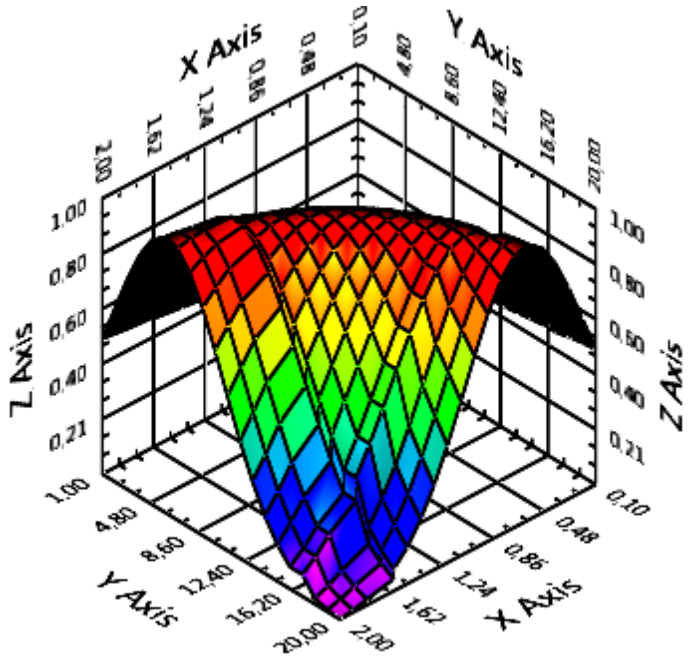


Рис. 3.24. Представлення d_{I_1} у вигляді безперервної тривимірної функції приналежності. Вісь Z відповідає функції бажаності Харрінгтона d ФК I_1; вісь X – значенням параметра J_1; вісь Y – значенням параметра J_2

Кроки 1…4 алгоритму визначення для ЛК збігаються з відповідними кроками алгоритму розрахунків для ФК.

Крок 5. По відомому коду метричної шкали Харрінгтона – розрахунок значення функції бажаності d_i для ППЯ які є критеріями і які на підставі дерева властивостей формують ЛК.

Крок 6. Згідно крокам 5…7 алгоритму для ФК, обчислення значення функції Харрінгтона для КПЯ які є фізичними критеріями і які на підставі дерева властивостей у якості квазіпростих ПЯ формують ЛК.

Крок 7. Розрахунок значення функції бажаності Харрінгтона для ЛК проводиться на підставі дерева властивостей з урахуванням значення функції Харрінгтона d_i простих і квазіпростих ПЯ, які формують ЛК [111]:

$$D = \sqrt[n]{\prod_{i=1}^{n} d_i}\,, \qquad (3.41)$$

де D − узагальнена функція бажаності Харрінгтона (функція бажаності ЛК що розглядається), n − кількість ПЯ, які формують ЛК.

Недоліком виразу (3.41) є те, що всі d_i рівноважні. Оскільки значення D згідно (3.41) є середнім геометричним, то для урахування ваг цей вираз можливо представити у вигляді середнього геометричного зваженого: $D = \sum_{i=1}^{n} w_i \sqrt{\prod_{i=1}^{n} d_i}$, де w_i − ваговий коефіцієнт i-го ПЯ. Детальний аналіз визначення вагових коефіцієнтів був проведений в [112], де показано, що їх значення лежать в діапазоні $0 < w_i \le 1$, а крок визначення складає 0,1. Причому найбільш вагомим коефіцієнтам присвоюється значення 1.

Розглянемо фрагмент дерева властивостей (рис. 3.21). Нехай вузол H_1 є логічним критерієм з нечітко заданими умовами. Тоді, відповідно до (3.41), $D = d_{H_1} = \sqrt{d_{I_1} \cdot d_{j_3}}$, де d_{j_3} − функція бажаності Харрінгтона критерію J_3 (простий показник), d_{I_1} − функція бажаності Харрінгтона критерію I_1 (квазіпростий показник). Представлення d_{H_1} у вигляді безперервної тривимірної функції приналежності, змодельоване у середовищі LabVIEW, приведене на (рис. 3.25).

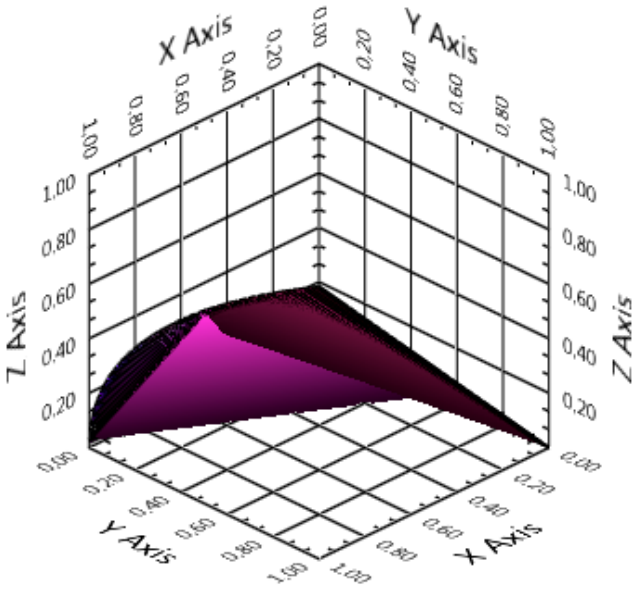


Рис. 3.25. Представлення d_{H_1} у вигляді безперервної тривимірної функції приналежності, де вісь Z відповідає функції бажаності Харрінгтона d_{H_1} ЛК H_1; вісь X - функції бажаності Харрінгтона d_{I_1} ФК критерію I_1; вісь Y – функції бажаності Харрінгтона d_{j_3} критерію J_3

Значення функції приналежності критеріїв визначаються як їхні цільові функції, в процесі парето-оптимізації. Теоретичне обґрунтування зв'язку парето-оптимальних розв'язків і векторів дані в [113]. Там же виведена рівність $P(Y) = f\left(P_f(X)\right)$, де $P(Y)$ − множина парето-оптимальних векторів, $f\left(P_f(X)\right)$ − множина парето-оптимальних розв'язків, та доведено, що знаючи множину парето-оптимальних розв'язків, можна знайти відповідну множину парето-оптимальних векторів і навпаки, маючи множину парето-оптимальних векторів можна побудувати відповідну множина парето-оптимальних розв'язків.

На підставі наведеного, можемо зробити висновок про те, що множину парето-оптимальних векторів можна розглядати як множину недомінуємих по відношенню $(\geq)$ елементів множини можливих векторів Y.

Приймемо Y за множину особин у популяції (множина багатомірних результуючих векторів критеріїв якості) $Y = \{y_1, y_2, ..., y_N\}$, де y_a − результуючий вектор a-ї особини, N − кількість особин у популяції . Використаємо в якості основи алгоритм побудови множини парето-оптимальних векторів (особин) з [113]. Після модифікації він матиме наступний вигляд:

Крок 1. Поклавши $P(Y) = Y$, $a = 1$, $b = 2$, утворюємо поточну множину парето-оптимальних векторів, яка на поточному кроці співпадає з множиною Y.

Крок 2. Реалізуємо перевірку виконання нерівності $y_a \geq y_b$ за кожним критерієм окремо, тобто зіставляємо довжини векторів відповідних критеріїв. Якщо нерівність неправильна, то здійснюємо перехід до кроку 5.

Крок 3. Видаляємо з поточної множини $P(Y)$ вектор y_b, оскільки він не є парето-оптимальним.

Крок 4. Перевіряємо виконання нерівності $b < N$. Якщо вона є істинною, то $b = b + 1$ і відбувається повернення до кроку 2. Якщо нерівність не є істинною, то відбувається перехід до кроку 7.

Крок 5. Перевіряємо нерівність $y_b \geq y_a$ за кожним критерієм окремо, тобто зіставляємо довжини векторів відповідних критеріїв. Якщо нерівність не є істинною, то відбувається повернення до кроку 4.

Крок 6. Видалення з поточної множини векторів $P(Y)$ вектора y_a.

Крок 7. Перевіряємо виконання нерівності $a \le N-1$. Якщо вона є істинною, то $a = a+1$, а потім $b = a+1$ та повернення до кроку 2. Якщо нерівність не є істинною, то відбувається закінчення обчислень.

У якості ознаки закінчення роботи генетичного алгоритму, як слідує з [113], найбільш часто використовують таке поняття, як «неполіпшення пристосованості популяції». У нашому випадку це означає *повторюваність парето-оптимальних векторів (особин) протягом декількох поколінь*.

Процес парето-оптимізації проводиться для кожної популяції, починаючи з початкової. Отримані парето-оптимальні особини використовуються для формування нової популяції в ГА, як основний генетичний матеріал. Аналіз ефективності різних методів відбору батьківських пар при багатокритеріальній оптимізації приведений у [114]. Варто відзначити, що в якості найбільш ефективних механізмів відбору у [114] відзначені *елітний, витиснення* та *ранговий*.

Завдання багатокритеріальної оптимізації показників якості ІВС може бути розв‘язане на основі мультихромосомного генетичного алгоритму, що дозволить знайти співвідношення параметрів елементів системи, які щонайкраще задовольняють заданим критеріям якості на всіх етапах життєвого циклу.

3.7. Проблематика якості інтернет-послуг, які надаються структурам сфери економіки

За даними Держкомстату в Україні налічується близько п’яти мільйонів Інтернет-користувачів, з них – близько 1 млн. 200 тис. складають абоненти, які відносяться до галузі економіки. Завдяки впровадженню нових технологій зі зниження вартості доступу, спостерігається стабільне збільшення числа таких користувачів. Так, наприклад, кожного року у першому кварталі їх кількість, в середньому, стабільно збільшується на 30% в порівнянні з аналогічним періодом попереднього року. У другому-четвертому кварталах цей показник є дещо меншим.

Одночасно із збільшенням кількості користувачів змінюються пріоритети їх запитів. Якщо до 2011 року основними видами Інтернет-трафіку були Web-серфінг та файловий обмін, який включав off-line-video, то після вказаної дати на перше місце вийшли мультимедійні та голосові програми.

Основним видом мультимедійного трафіку стало потокове відео, яке генерується тими ж файлообмінними та хмарними сервісами, Інтернет-телебаченням та системами відеоконференцій. Згідно з даними щорічного прогнозу компанії Cisco Systems (*CiscoVisual Networking Index Forecast*) до 2014 року обсяги Інтернет-трафіку зростуть у 4 рази відносно показників 2011 року. В цьому зростанні зіграє основну роль відеотрафік. В тому ж прогнозі зазначається, що протягом майбутніх 5 років кожен рік на частку відео-трафіку (у всіх форматах) припадатиме понад 90% глобального трафіку. Т.ч., як видно, проблематика якості послуг Інтернет-провайдерів є актуальною.

Аналіз останніх досліджень і публікацій показує, що передача мультимедійного трафіку має свої особливості пов’язані з рівнем якості надаваних сервісів – QoS (англ.: *Quality of Service* – якість обслуговування). Це положення відображене у документах МСЕ [115, 116]. У відповідності до них, Законом України «Про телекомунікації» та стандартами [117, 118] було встановлено 4 показники якості послуг при доступу до Інтернет:

1…3) швидкість передачі даних: найвища, найнижча та середня;

4) стандартне відхилення швидкості передачі даних.

Вченими та практикуючими фахівцями для цих показників якості послуг розробляються граничні рівні, конкретні значення яких повинні бути введені в дію відповідними розпорядженнями центрального органу виконавчої влади в галузі зв’язку. Попередній аналіз зазначених документів показує, що при наданні споживачеві послуги доступу в Інтернет договір між зацікавленими сторонами повинен містити показники якості, встановлені нормативними документами.

Договір про якість обслуговування є документом, який визначає взаємовідносини:

– абонентів з Інтернет-провайдером;

– провайдерів між собою;

– провайдерів з операторами зв’язку.

Виходячи з аналізу першоджерел нормативно-законодавчого спрямування, метою підрозділу є розгляд проблематики якості послуг Інтернет-провайдерів з точки зору їх відповідності нормативно-правовому базису.

Укладення вище зазначених договорів передбачено документом [119], де визначено поняття угоди про рівень обслуговування SLA (анг.: *Service Level Agreement*), і моделі диференціювання послуг – *DiffServ* (див. рис. 3.26).

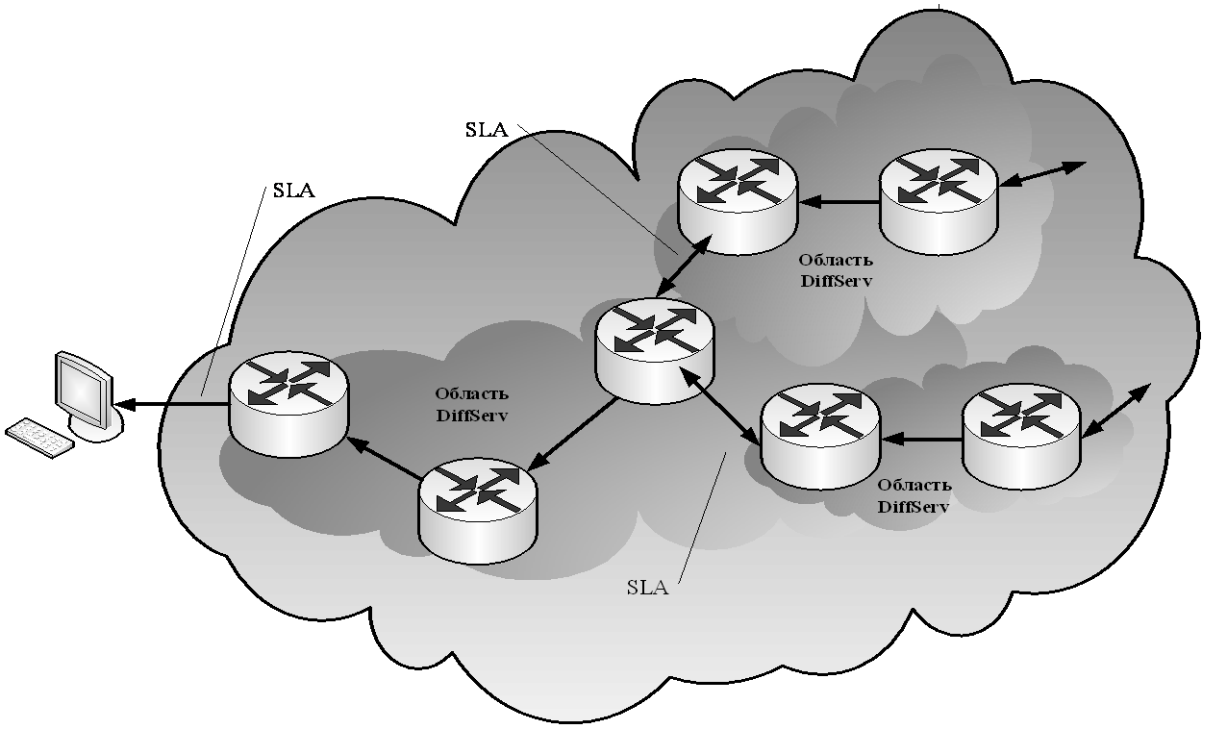


Рис. 3.26. Структура мережевої моделі *DiffServ*

Структура моделі, приведеної на рис. 3.26, включає в себе область *DiffServ*, яка належить до сфери впливу одного провайдера (або оператора зв’язку), та механізми обробки і проходження пакета по вузлах, що належить до цієї області. При цьому повинна зберігатися відповідна задана якість обслуговування.

У рамках диференціювання послуг відповідно до рекомендацій [116], для забезпечення необхідного рівня QoS передбачається розподіл наданих сервісів на 6 пріоритетних класів – залежно від необхідних значень характеристик передачі IP-пакетів. З них в якості основних можна виділити затримку доставки пакетів та варіацію затримки доставки (джіттер).

Найбільш критичними до параметрів передачі є сервіси реального часу (голосовий зв'язок, відеоконференц-зв'язок, Інтернет-телебачення), далі за важливістю – on-line перегляд відеофайлів та інтерактивна передача даних (веб-серфінг). Всі інші сервіси є терпимими до затримок. В зв'язку з цим їх відносять до найменш пріоритетних класів.

Аналіз якості надаваних сервісів Інтернет-провайдерами з точки зору абонента був проведений в Одеській області. Перша перевірка полягала в аналізі абонентських договорів, які в текстовому або інтерактивному вигляді були розміщені на сайтах найбільш великих провайдерів: Укртелеком, TeNeT, Vega та ін. Практично, в договорах всіх провайдерів, всупереч рекомендаціям [116-118], замість максимальної мінімальної та середньої швидкостей передачі, вказується (так, як це зроблено в рекламних проспектах) тільки максимально можлива швидкість: часто – з приставкою «до». Значення затримки та джиттера взагалі не фігурують. Втім це можна пояснити відсутністю вітчизняних нормативно-правових актів, які встановлюють граничні значення цих величин. Позитивним моментом є поява на сайтах провайдерів звітів про якість телекомунікаційних послуг – відповідно до вимог Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації (НКРЗ). На сьогоднішній день звіти стосуються тільки телефонного зв'язку, але з введенням в дію відповідних нормативних документів будуть відображати і якість послуг доступу до Інтернет. Це дозволить абонентам не тільки контролювати рівень надаваних сервісів, а й оптимізувати вибір провайдера.

Другий етап перевірки був заснований на аналізі реального трафіку, який надходить до абонента. Для цих цілей була побудована експериментальна

комп'ютерна мережа (див. рис. 3.27) для підключення до Інтернет-провайдера Vega. Тарифний план – «Безлімітний» до 10 Мбіт/с.

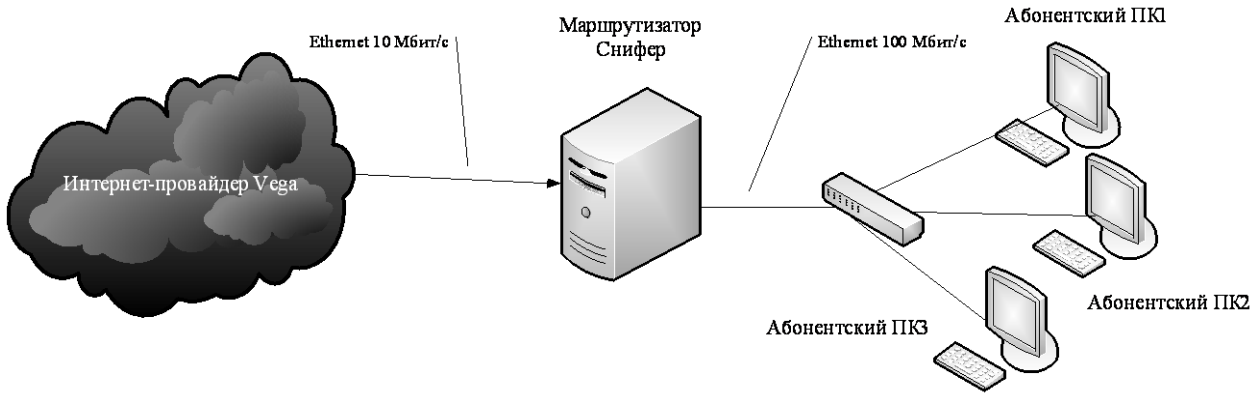


Рис. 3.27. Схема експериментальної комп'ютерної мережі

В якості маршрутизатора використовувався сервер з ОС SuSe Linux. Для перевірки був встановлений снифер Wireshark, що дозволило в реальному часі проводити збір пакетів, які поступали на мережевий інтерфейс. Досліджувався наступний мультимедійний трафік:

– on-line перегляд фільму з файлообмінного сервера FileShare;

– Інтернет-телебачення on-line-tv телеканалу Інтер;

– голосовий трафік Skype.

Кожен з сервісів надавався по запиту з окремого персонального комп'ютера. Реєстрація пакетів проходила на інтерфейсі підключення до провайдера таким чином, що внутрішня структура локальної мережі не чинила впливу на результат експерименту. У ході дослідження перевірялося відповідність QoS невисокоякісного мультимедійного трафіка рекомендаціям [116], а саме:

– затримка доставки IP-пакетів: не більше 400 мс;

– джиттер: не більше 50 мс.

Значення затримки Δt_i розраховувалися за формулою:

$$\Delta t_i = t_i - t_{i-1},$$

де t_i та t_{i-1} – час прибуття поточного та попереднього пакету, відповідно.

Джиттер τ_i розраховувався за формулою:

$$\tau_i = \left| t_{cp} - \Delta t_i \right|,$$

де t_{cp} – середнє значення затримки.

Результати досліджень приведені у табл. 3.2 та табл. 3.3; гістограми – на рис. 3.28.

Таблиця 3.2. Результати дослідження затримки доставки пакетів

Тип трафіку	Середнє значення	Максимальне значення	Відсоток пакетів з перевищенням граничного значення
Перегляд фільму	0,0012	0,676	0
Інтернет-телебачення	0,01	0,5	0,029
Голосовий зв’язок	0,02	2,73	0,046

Таблиця 3.3. Результати дослідження варіації затримки доставки пакетів

Тип трафіку	Середнє значення	Максимальне значення	Відсоток пакетів з перевищенням граничного значення
Перегляд фільму	0,0007	0,675	0
Інтернет-телебачення	0,017	0,489	3,63
Голосовий зв’язок	0,003	2,71	0,002

Аналіз результатів дослідження трафіку показав, що, не зважаючи на відсутність договірних зобов’язань щодо забезпечення QoS, характеристики трафіку, в основному, не виходять за межі граничних значень. Найгірші результати, як за візуальною оцінкою, так і за отриманими числовим значенням показав трафік Інтернет-телебачення, що є досить дивним, оскільки цей трафік відноситься до найбільш пріоритетного. Відповідь на це питання дає більш детальний аналіз пакетів, а саме – полів TOS (англ.: *Type of Service*) за-

головків IP-пакетів в яких якраз і вказується пріоритет трафіку. У всіх досліджених видах трафіку ці поля дорівнюють нулю. Таким чином, можна зробити висновок про те, що управління трафіком провайдера в області DiffServ, а також договори SLA між провайдерами, відсутні. Задовільні результати якості послуг досягаються лише за рахунок високої швидкості каналів передачі даних.

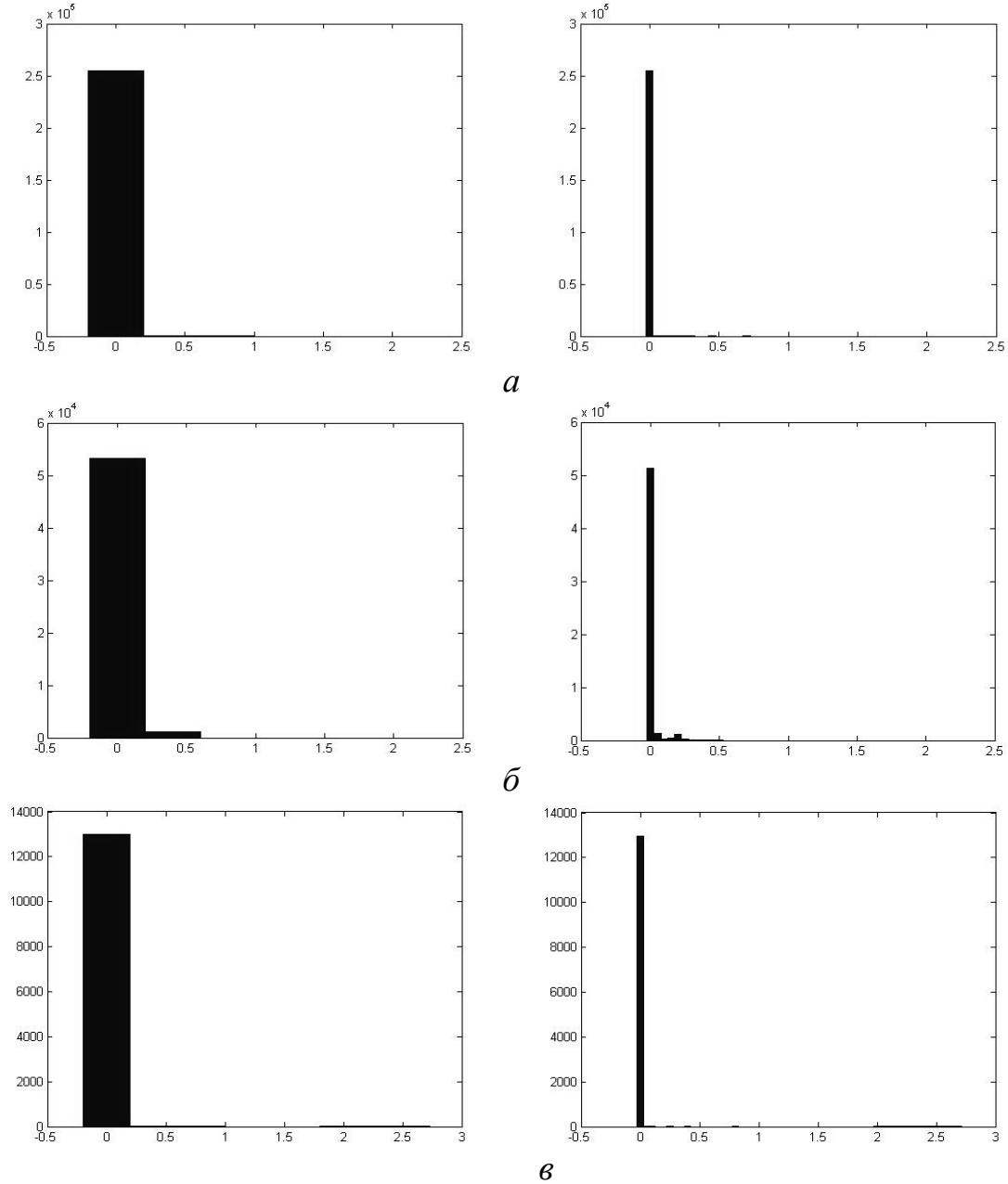


Рис. 3.28. Гістограми затримки та варіації затримки пакетів
(*а - перегляд фільму*, *б - Інтернет-телебачення*, *в - голосовий зв'язок*)

Зроблений висновок є орієнтовним, оскільки управління полями TOS може здійснюватися на будь-якому маршрутизаторі і, можливо, що на абонентському сегменті мережі значення поля змінюється.

До теперішнього часу забезпечення якості послуг Інтернету здійснювалося екстенсивними методами за рахунок збільшення пропускної здатності мереж. З ростом числа абонентів та зміни характеру трафіку така мережева політика призведе до зниження якості обслуговування. Найближчим часом ситуація може змінитися, оскільки центральні органи виконавчої влади в галузі зв’язку та НКРЗ вживають заходів щодо створення нормативно-правової бази стандартизує якість надання телекомунікаційних послуг.

Висновки до розділу 3

Встановлено, що одним з найбільш поширених в науці інформаційного права є уявлення про те, що при отриманні конфіденційної інформації відповідний режим таємниці трансформується з одного режиму в інший. При цьому відмічено, що відомості про діяльність будь-яких господарюючих суб'єктів та фізичних та юридичних осіб в цілому, які можуть бути предметом комерційної таємниці, функціонують в режимі, наприклад, банківської таємниці. Відповідно комерційна, професійна, банківська таємниця, персональні дані при наданні їх в органи державного управління не припиняють своє функціонування, а складають службові відомості, доступ до яких обмежений органами державної влади відповідно до діючого законодавства, так як до органів виконавчої влади надається не режим, а інформація.

Показано, що всередині підприємств та організацій сфери економіки, бізнесу та фінансів можуть функціонувати відомості, що становлять комерційну таємницю, персональні дані, різновиди професійної таємниці, щодо яких володар повинен забезпечити конфіденційність.

Відповідно до вище зазначеного, **визначено** питання, які можуть бути предметом подальшого вивчення та дослідження, а саме:

– які заходи для забезпечення конфіденційності повинні розробляти підприємства та організації сфери економіки, бізнесу та фінансів;

– чи повинні організації та підприємства в обов'язковому порядку встановлювати режим комерційної таємниці;

– забезпечення режиму захисту персональних даних;

– забезпечення режиму професійної таємниці.

Науковою новизною дослідження є:

– встановлення того факту, що режим конфіденційності інформації у сфері економіки, бізнесу та фінансів є предметом правового регулювання, яке представляє особливий порядок, встановлений державою у вигляді правових норм і забезпечений силою державного примусу за допомогою застосування

будь-яких дій з інформацією конфіденційного характеру, включаючи збір, систематизацію, накопичення, зберігання, уточнення, оновлення, зміни, використання, розповсюдження (у тому числі передачу), блокування, знищення;

– для забезпечення конфіденційності однієї і тієї ж інформації існує можливість встановлювати різні режими, які, втім, можуть привести до виникнення конфліктів інтересів суб'єктів таємниць. Для виключення конфліктів при здійсненні інформаційного обміну показана доцільність закріплення в нормативних актах поняття «режим конфіденційності інформації», який дозволив би встановити єдині правила та вимоги до забезпечення безпеки інформації як в органах державної влади, так і господарюючих суб'єктів.

Практичним значенням отриманих результатів є те, що:

– на основі оцінки ризиків можливе виявлення загроз активам, оцінка уразливості відповідних активів і ймовірності виникнення загроз, а також оцінка можливих наслідків;

– використання законодавчих вимог для забезпечення узгодженості, цілеспрямованості, планомірності діяльності щодо забезпечення інформаційної безпеки веде до підвищення рівня захищеності будь-якого підприємства сфери економіки, бізнесу та фінансів;

– з'явилася можливість визначення адекватності заходів захисту з урахуванням принципу оптимальності витрат на захист інформації.

Отримані результати, у відповідності до вище зазначених наукової новизни та практичного значення, відповідають рівню аналогічних розробок, отриманих науковими приацівниками та вченими світового рівня. Їх достовірність, точність та коректність підтверджені достатньою кількість наукових публікацій у виданнях за переліками ВАК України та у виданнях, що входять до міжнародних науковометричних баз даних. За результатами досліджень опубліковану 1 монографію та отримано 1 патент на винахід.

ЗАГАЛЬНІ ВИСНОВКИ

Огляд та аналіз поточного стану технологій ідентифікації та управління доступом, а також перспективи використання їх у сучасних системах захисту інформації на підприємствах та організаціях сфери економіки, бізнесу та фінансів, показав наступне:

1) Задача аналізу, переробки та відображення візуальної інформації, як завдання щодо розвитку та створення пристроїв ідентифікації особи абонента з використанням біометричних даних в цілях захисту інформації від несанкціонованого використання або навмисного спотворення, відноситься до проблем, які вирішуються у рамках теорії розпізнавання образів.

2) Визначено місце завдання ідентифікації особи абонента на основі використання його біометричних даних у загальній схемі функціонування технологічної системи, яка використовує систему захисту інформації (СЗІ) та технології прогнозування стану при виникненні в ній інцидентів.

3) Виділені основні поняття теорії розпізнавання образів, які можуть бути використані при розробці положень щодо створення пристроїв ідентифікації особи абонента з використанням біометричних даних в цілях захисту інформації.

4) Показано, що не зважаючи на загальну негативну оцінку сучасного стану біометричних систем ідентифікації особистості, спостерігається тенденція до розвитку досліджень та розробок в області біометрії. При цьому однією з основних тенденцій є поступовий перенос пріоритетів з контактних на безконтактні методи біометричного розпізнавання.

5) Виділено три групи специфічних проблем, які не мають адекватного роз’язку у сенсі створення біометричних систем нового покоління. На основі їх аналізу показана необхідність комплексування результатів біометричного розпізнавання, отриманих від різних джерел інформації.

6) Виділено 2 напрямки, які існують у практиці розпізнавання образів. Базуючись на них, стосовно задач, які вирішуються в НДР, обрано той, що

розвиває теоретичні принципи та практичні методи побудови пристроїв, призначених для вирішення окремих завдань СЗІ в прикладних цілях.

7) Виділено 4 напрямки, які існують у практиці досліджень проблеми розпізнавання осіб. З врахуванням п. 6, обрано напрямок, який є комплексним та базується на дослідженні інформаційно-процесуальних моделей зі створенням комп'ютерних моделей розпізнавання.

8) Виконано формальну постановку завдання до НДР у сенсі змісту розділу 1 щодо управління ідентифікаційною інформацією і доступом, яке поягає в удосконаленні та підвищенні ефективності методів та технологій, які забезпечують процедуру аутентифікації у СЗІ на основі використання біометричних технологій для підприємств та організацій сфери економіки, бізнесу та фінансів.

9) Розроблено загальну схему дослідження, якою передбачено використання логічних розмірковувань та адекватиних математичних доказів. Схема відповідає класичній постановці задачі розпізнавання образів у системах забезпечення спостереженості.

10) Проведено огляд та вибір інформативних ознак зображень для розв'язку задачі біометричної ідентифікації особи, а також вибір предмета та технології розпізнавання. Як результат показано, що розв'язком проблеми вибору інформативних ознак для систем біометричної ідентифікації, може бути використання системи ознак, яка базується на побудові одномірних гістограм. При цьому, з посиланням на матеріали наступних розділів, виділена необхідність попередньої обробки зображень з метою поліпшення якості розпізнавання та його ймовірності.

Визначення та обґрунтування
патенто- і ліцензійно спроможних результатів

На поточному етапі досліджень патенто- і ліцензійно спроможних результатів з удосконалення та підвищення ефективності методів та технологій, які забезпечують процедуру аутентифікації у СЗІ на основі використання біометричних технологій не отримано.

**Нові конкурентоспроможні товари та послуги,
які будуть або вже створені на базі результатів роботи**

Нові конкурентоспроможні товари та послуги для підприємств та організацій сфери економіки, бізнесу та фінансів, на базі результатів роботи будуть визначатися та встановлюватися на останньому етапі НДР.

**Інвестиційна привабливість, обґрунтований економічний,
соціальний та інший ефект результатів роботи**

Інвестиційна привабливість, обґрунтований економічний, соціальний та інший ефект результатів досліджень для підприємств та організацій сфери економіки, бізнесу та фінансів, будуть визначатися та встановлюватися на останньому етапі НДР.

**Підприємства, організації, установи, заклади,
що впроваджують результати, шляхи просування на ринок**

Підприємства, організації, установи та заклади сфери економіки, бізнесу та фінансів, що впроваджують результати, а також шляхи їх просування на ринок, будуть визначатися та встановлюватися на третьому та четвертому етапах НДР.

Використання результатів у навчальному процесі (1 етап НДР)
Нові спеціальності, спеціалізації, курси лекцій або їх розподіли, практичні та лабораторні роботи, які (будуть) започатковані на основі результатів цього наукового дослідження в навчальному процесі

На основі результатів наукових досліджень, проведених на 1 етапі НДР, стосовно розділу «Управління ідентифікаційною інформацією і доступом», для навчального процесу кафедри:

– 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 у виданій монографії за темою дослідження, можуть бути використані при підготовці бакалаврів спеціальності 8.18010014 «Управління фінансово-економічною безпекою» кваліфікації «Професіонал з фінансово-економічної безпеки» та «Аналітик з питань фінансово-економічної безпеки».

Перелік докторських і кандидатських дисертацій, що захищені та підготовлені на базі науково-дослідної роботи за час її виконання
(найменування дисертації, докторська чи кандидатська, автор, науковий керівник або консультант, для захищених – дата захисту)

На базі науково-дослідної роботи виконуються та готуються до захисту:

1) докторські дисертації

– «Розвиток теорії та удосконалення принципів багаторівневого захисту інфор-мації у недовірених системах» (ДСК), автор канд. техн. наук, доц. Казакова Н.Ф., науковий консультант докт. техн. наук, доц. Скопа О.О.;

– «Теорія вирішення завдань забезпечення фінансово-економічної безпеки на основі системного аналізу і нечіткого когнітивного моделювання» (ДСК), автор канд. екон. наук, доц. Орлик О.В., науковий консультант докт. техн. наук, доц. Скопа О.О.

2) кандидатські дисертації

– «Підвищення ефективності методів забезпечення превентивної безпеки у системах з обмеженим доступом» (ДСК), автор ст. викл. Фразе-Фразенко О.О., науковий керівник канд. техн. наук, доц. Казакова Н.Ф.;

– «Удосконалення методів забезпечення захисту персональних даних у системах Інтернет-банкінгу» (орієнтовна тема), автор ст. викл. Єсіна О.Г., науковий керівник канд. техн. наук, доц. Казакова Н.Ф.;

– «Удосконалення технологій інтерпретації ризик-орієнтованих оцінок інформаційної безпеки» (орієнтовна тема), автор викл. Йона О.О., науковий керівник докт. техн. наук, доц. Скопа О.О.

Кількість курсових, дипломних та інших робіт, що захищені на базі зазначеної наукової роботи за час її виконання

Виконання курсових, дипломних та інших робіт на базі наукової роботи не передбачається навчальними планами напрямів та спеціальностей у зв‘язку з тим, що кафедра не є випускною.

Використання результатів у науковій роботі, науково-технічній та інноваційній діяльності студентів, в інших закладах освіти

Результати, отримані при виконанні НДР, використовуються у науковій роботі, науково-технічній та інноваційній діяльності студентів при проведенні студентських олімпіад та конференцій з документуванням їх у протоколах засідання секцій.

Т.ч., виходячи з вище викладеного, при виконанні 1-го етапу НДР розроблені та удосконалені окремі методології, 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: з управлінням ідентифікаційною інформацією і доступом; управлінням інформаційною та фінансово-економічною безпекою підприємств; зі збереженням конфіденційності та захистом даних.

СПИСОК ЛІТЕРАТУРНИХ ПЕРШОДЖЕРЕЛ

1. Горбатюк, О. М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть [Текст] / О. М. Горбатюк // Вісник Київського університету імені Т. Шевченка. – 1999. – № 14 : Міжнародні відносини. – С. 46-48.
2. Баринов, А. Информационный суверенитет или информационная безопасность? [Текст] / А. Барсуков // Національна безпека і оборона. – 2001. – № 1. – С. 70-76.
3. Бучило, И. Л. Информационное право: основы практической информации [Текст] : монографія / И. Л. Бучило. – М., 2001. – 253 с.
4. Борсуковский, Ю. Подходы и решения : Информационная безопасность [Текст] / Ю. Борсуковский // Мир денег. – 2001. – № 5. – С. 41-42.
5. Щербина, В. М. Інформаційне забезпечення економічної безпеки підприємств та установ [Текст] / В. М. Щербина // Актуальні проблеми економіки. – 2006. – № 10. – С. 220-225.
6. Березюк, Л. П. Организационное обеспечение информационной безопасности [Текст] : навч. посібник / Л. П. Березюк. – Хабаровськ : ДВГУПС, 2008. – 188 с.
7. Игнатьев, В. А. Информационная безопасность современного коммерческого предприятия [Текст] : монографія / В. А. Игнатьев. – Старий Оскол : ООО «ТНТ», 2005. – 448 с.
8. Маракова, І. Захист інформації [Текст] : підручник / Маракова І., Рибак А., Ямпольский Ю. – Одеса : ОдНПУ, 2001. – 164 с.
9. Захаров, Е. Информационная безопасность или опасность отставания? [Текст] / Е. Захаров // Права людини. – 2000. – № 1 . – С. 3-5.
10. Про інформацію : закон України [Текст] : [закон України : офіц. текст: за станом на 02 жовтня 1992 року]. – К.. : Парламентське вид-во, 1996. – Т.4.
11. Про захист інформації в автоматизованих системах : закон України [Текст] : [закон України : офіц. текст: за станом на 05 липня 1994 року]. – К.. : Парламентське вид-во, 1996. – Т.7.
12. Литвиненко, О. Інформація і безпека [Текст] / О. Литвиненко // Нова політика. – 1998. – № 1. – С. 47-49.
13. Горбатюк, О. М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть [Текст] / О. М. Горбатюк // Вісник Київського університету імені Т. Шевченка. – 2009. – № 14 : Міжнародні відносини. – С. 46-48

14. Остроухов, В. В. До проблеми забезпечення інформаційної безпеки України [Текст] / В. В. Остроухов // Політичний менеджмент. – 2008. – № 4. – С. 135–141.

15. Павлидис, Т. Алгоритмы машинной графики и обработки изображений [Текст] / Т. Павлидис. – М. : Радио и связь, 1986. – 394 с. – ISBN відсутній : [Електронний ресурс] // Портал : eknigu.com. – Режим доступу \www/ URL: http://www.eknigu.com/info/Cs_Com puter_20 science/CsIp_Image_20processing/Pavlidis_20T._20 Algorit my_ 20mashinn oj_ 20grafiki_20i_20obrabotki_ 20izobrazhe nij _20 (RiS,_201986)(ru)(K)(T) (394s)_CsIp_.djvu#a. – Заголовок з документа, доступ вільний, 14.01.2013.

16. Искусственный интеллект. Книга 1. Системы общения и экспертные системы : довідник / коллект. авторов ; под. ред. Э. Попова. – М. : Радио и связь, 1990. – 464 с. – ISBN 5-256-00365-8 (кн. 1) : [Електронний ресурс] // Портал : без назви. – Режим доступу \www/ URL: http://www. twirpx. com/file/218565. – Заголовок з документа, доступ вільний, 14.01.2013.

17. Александров, В. В. Алгоритмы и программы структурного метода обработки данных : монография / В. В. Александров, Н. Д. Горский. – Л. : Наука, 1983. – 208 с. – ISBN відсутній.

18. Александров, В. В. Базы видеоданных: проблемы и перспективы : монография / В. В. Александров, Н. Д. Горский. – Л. : ЛНИВЦ, 1985. – 72 с. – ISBN відсутній.

19. Александров, В. В. Представление и обработка изображений. Рекурсивный подход : монография / В. В. Александров, Н. Д. Горский. – Л. : Наука, 1985. – 192 с. – ISBN відсутній.

20. Common Criteria [Електронний ресурс] / Портал : Вільна енциклопедія. – Режим доступу \www/ URL: http://uk.wikipedia.org/wiki/ Common_ Criteria#.D0.A1.D0.BF.D0.BE.D1.81.D1.82.D0.B5.D1.80. D0.B5.D0.B6.D0.B5.D0.BD.D1.96.D1.81.D1.82.D1.8C. – Заголовок з екрану, доступ вільний, 14.01.2013.

21. Bonsor, K. How Facial Recognition Systems Work [Електронний ресурс] / K. Bonsor, R. Johnson // Портал : Howstuffworks – Режим доступу \www/ URL: http://electronics.howstuffworks.com/gadgets/ high-tech-gadgets/facial-recognition.htm. – Заголовок з екрану, доступ вільний, 15.01.2013.

22. Цифровая обработка сигналов в оптике и голографии : Введение в цифровую оптику [Текст] / Л. П. Ярославский. – М. : Радио и связь, 1987. – 296 с. : ил., табл. – Библиогр. : с. 291–294. – ISBN відсутній.

23. Александров, В. В. ЭВМ видит мир : монография / В. В. Александров, Н. Д. Горский. – Л. : Машиностроение, Ленингр. отд-ние, 1990. – 136 с. – ISBN відсутній.

24. Распознавание лиц [Електронний ресурс] / Портал : Википедия. – Режим доступу \www/ URL: http://ru.wikipedia.org/wiki/Распознавание_лиц. – Заголовок з екрану, доступ вільний, 16.10.2012.

25. Колодникова, Н. В. Обзор текстурных признаков для задач распознавания образов [Текст] / Н. В. Колодникова // Доклады ТУСУР : Автоматизированные системы обработки информации, управления и проектирования. – 2004. – БН. – С. 113-124. – ISSN відсутній. – [Електронний ресурс] / Портал : tusur.ru. – Режим доступу \www/ URL: www.tusur.ru/filearchive/ reports-magazine/2004-9-1/113.pdf. – Заголовок з контейнера, доступ вільний, 23.04.2013.

26. Спектральный анализ меридиональной системы [Електронний ресурс] / Портал : tusur.ru. – Режим доступу \www/ URL: http:// skfb.ru/ p110 aa1.html. – Заголовок з екрану, доступ вільний, 23.04.2013.

27. Традиционные методы биометрической аутентификации и идентификации : навчальний електронний посібник / Колешко В. М., Воробей Е. А., Азизов П. М. [та ін.]. – Минск : БНТУ, 2009. – 107 с. – ISBN відсутній. – [Електронний ресурс] / Портал : BNTU. – Режим доступу \www/ URL: rep.bntu.by/bitstream/data /780/7/ Основной% 20текст.pdf. – Заголовок з контейнера, доступ вільний, 24.04.2013.

28. Протасов, К. Т. Непараметрический алгоритм распознавания объектов подстилающей поверхности Земли по данным аэрокосмической съемки [Текст] / К. Т. Протасов, А. И. Рюмкин // Вестник Томского государственного университета. – 2002. – №275. – С. 41-46. – ISSN відсутній.

29. Андреев, Г. А. Анализ и синтез случайных пространственных текстур [Текст] / Г. А. Андреев, О. В. Базарский, А. С. Глауберман та ін. // Зарубежная радиоэлектроника. – 1984. – №2. – С. 3-33. – ISSN відсутній.

30. Харалик, Р. М. Статистический и структурный подходы к описанию текстур [Текст] / Р. М. Харалик // ТИИЭР. – 1979. – Т.67. – №5. – ISSN відсутній.

31. Потапов, А. А. Новые информационные технологии на основе вероятностных текстурных и фрактальных признаков в радиолокационном обнаружении малоконтрастных целей [Текст] / А. А. Потапов // Радиотехника и электроника. – 2003. – Т.48. – №9. – С. 1101-1119. – ISSN відсутній.

32. Сергеев, В. В. Параллельно-рекурсивные КИХ-фильтры для обработки изображений [Текст] / В. В. Сергеев // Компьютерная оптика. – 1992. – №10-11. – С.186-201. – ISSN відсутній.

33. Напрюшкин, А. А. Алгоритмическое и программное обеспечение системы интерпретации аэрокосмических изображений для решения задач картирования ландшафтных объектов : Дис.... канд. техн. наук. – Томск, 2002. – 183 с.

34. Цифровая обработка изображений : в 2 кн., пер. с англ. / У. Прєтт. – М. : Мир, 1982. – 790 с. – ISBN 978-5-94836-122-2.

35. Обиралов, А. И. Дешифрирование снимков для целей сельского хозяйства : навчальний посібник / А. И. Обиралов. – М. : Недра, 1982. – 144 с. – ISBN відсутній.

36. Вишневский, В. В. Структурный анализ цифровых контуров изображений как последовательностей отрезков прямых и дуг кривых [Текст] / В. В. Вишневский, В. Г. Калмыков // Штучний інтелект. – 2004. – №3. – С. 479-488. – ISSN відсутній.

37. Калмыков, В. Г. Структурный метод описания и распознавания отрезков цифровых прямых в контурах бинарных изображений / В. Г. Калмыков // Штучний інтелект. – 2002. – №4. – С. 450-457. – ISSN відсутній.

38. Загоруйко, Н. Г. Методы распознавания и их применение : монографія / Н. Г. Загоруйко. – М. : Советское радио, 1972. – 208 с. – ISBN відсутній.

39. Pushkareva, T.G. Detection of fires from satellite images using a nonparametric algorithm of pattern recognition in space of the informative parameters [Текст] / T. G. Pushkareva, K. T. Protasov // Proceedings of SPIE. – 2000. – V. 4341. – С. 283-285. – ISSN відсутній.

40. Кормилицына И. Г. Финансовая стабильность: сущность, факторы, индикаторы [Електронний ресурс] / Портал : Финансы и кредит. – Режим доступа \www/ URL: http://www.fin-izdat.ru/ journal/ fc/detail. php?ID=43883. – Финансы и кредит, 2011. – №35(467). – С. 44-54. – Заглавие из текста, доступ свободный, 10.10.2012.

41. Арсентьев М. Финансовая безопасность России [Електронний ресурс] / Портал : Проблемы безопасности России. – Режим доступа \www/ URL: http://www.rau.su/observer/N08_00/08_21.htm. – Заглавие с экрана, доступ свободный, 12.10.2012.

42. Овчинникова А. В. Экономический рост в рамках устойчивого развития социально-эколого-экономической системы [Електронний ресурс] / Портал : Экономика и право. – Режим доступа \www/ URL: http://www. vestnik.udsu.ru/2012/2012-022/vuu_12_022_08. pdf. – Заглавие из текста, доступ свободный, 10.10.2012.

43. Ткаченко В. Г. Об особенностях финансовой безопасности Украины в условиях рыночных трансформационных процессов [Електронний ресурс] / Режим доступа \www/ URL: http://www.nbuv. gov.ua/portal/ soc_gum/e_apk/2009_6/09_06_01.pdf. – Заглавие из текста, доступ свободный, 12.10.2012.

44. Ивашина, С. Ю. Инфраструктура социализации экономики [Текст] / С. Ю. Ивашина // Бизнес-информ. – Х. : ХНЭУ. – 2012. – № 6. – С. 13-17.

45. Коваленко Е. В. Экономическая безопасность регионов в социально-экономическом контексте [Електронний ресурс] / В.Г. Ткаченко, Е.В Коваленко // Режим доступа \www/ URL: http:// www. nbuv.gov. ua/portal/soc_ gum/vchu/N151/N151p129-135. pdf. – Заглавие из текста, доступ свободный, 12.10.2012.

46. Столбов, М. И. Финансовый рынок и экономический рост: контуры проблемы [Текст] : монография / М.И. Столбов // М. : Научная книга, 2008. – 201 с. – (Россия в мировой экономике). – ISBN 978-5-91393-007-1.

47. Доклад о человеческом развитии 2011. Устойчивое развитие и равенство возможностей: лучшее будущее для всех [Електронний ресурс] / Режим доступа \www/ URL: http://www.hdr.undp.org/en/ media/HDR_2011_RU_Complete.pdf. – Заглавие из текста, доступ свободный, 12.10.2012. – Опубликовано для Программы развития Организации Объединенных Наций (ПРООН).

48. Терентьев А.М., Ляпичева Н.Г., Кочетова Н.А. Мониторинг корпоративной сети ЦЭМИ РАН в условиях использования коммутатора Cisco Catalyst-2924 / Развитие и использование средств сетевого мониторинга и аудита. – Вып. 1. – Сборн. статей под ред. А.М. Терентьева – М. : ЦЭМИ РАН, 2004. – С. 75-87.

49. Жуков А.В., Аминова И.В. Исследование сетевого трафика web-ресурса «Петрозаводский государственный университет» / [Электронный ресурс] : www.energy-links.com (Режим доступа – свободный).

50. Кочетова Н.А., Ляпичева Н.Г. Методы и средства защиты магистральных маршрутизаторов и серверов удаленного доступа производства Cisco Systems / Вопросы информационной безопасности узла Интернет в научных организациях : Сборник статей под ред. М.Д. Ильменского. – М. : ЦЭМИ РАН, 2001. – С.10-42.

51. Хорошко В.А., Шелест М.Е., Маракова И.И., Сыропятов А.А. Защита информации в беспроводных системах связи // Захист інформації. – К.: ДУІКТ. – 2005. – №3 (25) – С. 83- 91.

52. Потапов М.В., Сиропятов А.О., Оценка эффективности информационной защиты комплексных систем связи // Управління проектами та розвиток виробництва: Вісник СНУ ім. В. Даля. – Луганськ : СНУ ім. В. Даля. – 2006. – 7 стор.

53. Маракова И.И., Скопа А.А., Сыропятов А.А. Комплексная защита информации в беспроводных системах связи // Матер. IV наук.-конф. Департамента спец. телеком. систем та захисту інформ. та Служби безпеки «Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні». – К. : НДЦ «Тезис» НТУУ «КПІ». – 2007. – С.73-75.

54. Казакова Н.Ф. Апріорна суперечність раціональної концепції інтелектуальної мережі / Управління проектами: стан та перспективи: Матер. міжнар. наук.-техн. конф. – Миколаїв : НУК ім. адмірала Макарова, 2008. – С.65-67.

55. Казакова Н.Ф., Годулян И.О., Чуприна А.А. Анализ эффективности информационных систем путем синтеза критериев оптимизации алгоритмов их функционирования / Матер. II наук.-практ. семін. молодих науковців та студентства «Сучасні телекомунікаційні та інформаційні технології», 12-14 грудня 2007 р., К. : УНДІЗ.

56. Казакова Н.Ф., Согіна Н.М. Скорочення обсягів контрольних випробувань в інформаційних системах за рахунок їх функціональної надмірності / Моделювання та інформаційні технології. Зб. наук. праць ІПМЕ НАН України. – Вип. 49. – К. : 2008.

57. Казакова Н.Ф., Годулян И.О., Чуприна О.О. Установление критериев оптимизации алгоритмов при определении эффективности информационных систем / Наукові записки УНДІЗ. – №1. – К. : УНДІЗ, 2007. – С.62-71.

58. Казакова Н.Ф. Методика организации идеального профилактического обслуживания // Под ред. В.В. Шахгильдяна / Матер. науч.-техн. семин. «Системы синхронизации, формирования и обработки сигналов для связи и вещания», 1-4 июня 2007 г., Москва-Одесса : IEEE-РНТОРЭС им.А.С.Попова. – С.167-172.

59. Казакова Н.Ф. Управління послугами телекомунікацій // 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.18-21.

60. Казакова Н.Ф. Задачі захисту інформаційних ресурсів від впливу зовнішніх загроз // Матер. II молод. наук. конф. «Сучасні інформаційні технології в повсякденній діяльності та підготовці фахівців», 31 березня 2006 р., Одеса : ОНЮА, 2006.

61. Казакова Н.Ф. Аналіз внутрішніх та зовнішніх загроз корпоративних мереж // Матер. міжвідомч. міжрегіон. семінару Наук. Ради НАН України «Технічні засоби захисту інформації», 15 лютого 2006 р., Київ-Одеса : НАН України, 2006. – С.11.

62. Щербина Ю.В., Казакова Н.Ф. Проблемы объективной оценки параметров защищенных автоматизированных систем // Матер. IV наук.-техн. конф. «Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні», 1-3 березня 2006 р., К. : НТУУ «КПІ», 2006. – С.60-61.

63. Казакова Н.Ф. Принципи створення систем мережного управління // Матер. наук.-практ. конф. проф.-викл. складу «Актуальні проблеми та досвід використання сучасних інформаційно-комунікаційних технологій», 10-12 травня 2005 р., Одеса : ОНЮА, 2005. – С.133-138.

64. Казакова Н.Ф. Особенности расчета показателей надежности компьютерных устройств управления резервным оборудованием // Матер. VI Міжнар. наук.-практ. конф. студентів, аспірантів та молодих вчених ІПСА-2004 «Системний аналіз та інформаційні технології», 1-3 липня 2004 р., К. : НТУУ «КПІ», 2004. – С.209-210.

65. Kazakova N. Mobil radio-service management system construction principles // 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.

66. Казакова Н.Ф. Аналіз моделей побудови мереж зв'язку з радіодоступом // Тр. II междунар. научно-практ. конф. «Современные информационные и электронные технологии СИЭТ-2001» : 28-31 мая 2001 г. – Одесса : ОдГПУ. – 2001. – С.66-67.

67. Казакова Н.Ф. Інформаційне забезпечення системи управління якістю продукції в сфері телекомунікацій // Тр. IV Междунар. научно-практ. конф. «Системы и средства передачи и обработки информации»: ОАО «Нептун», УГАС им.А.С.Попова, Одесса, 6-14 сент. 2000 г. – Одесса, 2000. – С.59-61.

68. A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications. NIST Special Publication 800-22. May 15, 2001.

69. The Marsaglia Random Number CDROM including the Diehard Battery of Tests of Randomness // http:// www.stat.fsu.edu/pub/ diehard/ Statistical test suite Crypt-X //http://www.isi.qut.edu.au/resources/ cryptx.

70. eSTREAM, the ECRYPT Stream Cipher Project [Електронний ресурс] // Портал : без назви. – Режим доступу \www/ URL : http://

www.ecrypt.eu.org/stream/index.html. – Заголовок з екрану, доступ вільний, 18.05.2013.

71. Кнут, Д. Искусство программирования для ЭВМ [Текст] : монография / Д. Кнут. – М. : Мир, 1977. – 727 с.

72. Харин, Ю. С. Математические и компьютерные основы криптологии [Текст] : учебное пособие / Ю. С. Харин, В. И. Берник, Г. В. Матвеев, С. В. Агиевич. – М. : Новое издание, 2003. – 272 с.

73. Земор, Ж. Курс криптографии [Текст] : монография / Ж. Земор. – Ижевск : НИЦ «Регулярная и хаотическая динамика»; Институт компьютерных исследований, 2006. – 256 с.

74. Рябко, Б.Я. Криптографические методы защиты информации [Текст] : учебное пособие / Б. Я. Рябко, А. Н. Фионов. – М. : МГУ, 2005. – 115 с.

75. Фомичев, В. М. Дискретная математика и криптология [Текст] : курс лекций / В. М. Фомичев // под общ. ред. Н. Д. Подуфалова. – М. : ДИАЛОГ-МИФИ, 2003. – 400 с.

76. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си [Текст] : монография / Б. Шнайер. – М. : Триумф, 2002. – 816 с.

77. Кац, М. Статистическая независимость в теории вероятностей, анализе и теории чисел [Текст] : монография / М. Кац. – М.: Издательство иностранной литературы, 1963. – 156 с.

78. Скопа О.О. Інтервальне оцінювання надійності Т-систем з паралельним з'єднанням елементів за результатами їх біноміальних іспитів // Наукові праці ОНАЗ: Період. наук. збір. з радіотехніки і телекомунікацій, електроніки та економіки в галузі зв'язку. – Одеса, 2002. – №1. – С.65–71.

79. Казакова Н.Ф., Мухін О.М., Скопа О.О. Скорочення обсягу випробувань систем телекомунікацій на надійність за рахунок їх структурної надмірності // 1–й Междунар. радиоэлектрон. форум «Прикладная радиоэлектроника. Состояние и перспективы развития»: 8–10 октября 2002 г.: Сб. научн. трудов. – Харьков: ХНУРЭ. – 2002. – С.358–360.

80. 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.

81. Скопа О.О., Казакова Н.Ф., Мурін О.С. Вплив функціональної надмірності резервованих систем телекомунікацій на скорочення обсягів їх випробувань на надійність // Наук. праці ДонНТУ. Серія:

Обчислювальна техніка та автоматизація. Випуск 58. – Донецьк: РВА ДонНТУ, 2003. – С.115-121.

82. Скопа О.О. Обслуговування резервних систем зв'язку // Наук. праці ДонДТУ. Серія: Обчислювальна техніка та автоматизація. Випуск 38. – Донецьк: РВА ДонДТУ, 2002. – С.89-91.
83. Скопа О.О. Оптимізація експлуатації резервних систем телекомунікацій // Праці УНДІРТ. – Одеса, 2002. – №1(29). – С.91–93.
84. Скопа О.О. Інтервальне оцінювання надійності Т-систем з паралельним з'єднанням елементів за результатами їх біноміальних іспитів // Наукові праці ОНАЗ: Період. наук. збір. з радіотехніки і телекомунікацій, електроніки та економіки в галузі зв'язку. – Одеса, 2002. – №1. – С.65–71.
85. Скопа А.А., Казакова Н.Ф. Применение теории псевдополуобратных матриц к решению задач по оценке надежности систем телекоммуникаций. Часть 1. Общие положения // Праці УНДІРТ. – Одеса, 2002. – №4(32). – С.88-91.
86. Казакова Н.Ф. Технічне рішення задачі Клопера-Пірсона / Наук. записки Міжнар. гуманіт ун-ту. Випуск 3. – Одеса: МГУ, 2005. – С.89-94.
87. Казакова Н.Ф. Аналітичне розв'язання одновимірної задачі Клопера-Пірсона // Радиотехника: Всеукр. межведомств. научн.-техн. сб. – Харьков: ХНУРЭ. – 2002. – Вып. 128. – С.97-98.
88. Бурбаки Н. Теория множеств. – М.: Мир, 1965. – 465 с.
89. Судаков Р.С. Интервальная оценка монотонных функций по результатам испытаний // Техническая кибернетика. Изв. АН СССР. – 1986. – №1. – С. 82-91.
90. Судаков Р.С., Северцев Н.А. и др. Статистические задачи отработки систем и таблицы для числовых расчетов показателей надежности. – М.: Высшая школа, 1975. – 607 с.
91. Харди Г., Литтлвуд Д., Полиа Г. Неравенства. – [Электронный ресурс]: http://e-books.enigma.uran.ru/book_djvu/hardi/hardi.djvu: Доступ свободный.
92. Обратные и некорректные задачи // Наука в Сибири: Еженедельная газета Сибирского отделения РАН. – №40(2725), 08.10.2009. – [Електронний ресурс]: http://www-sbras.nsc.ru/HBC/ article.phtml? nid =519&id=10. – Режим доступу: вільний.
93. Кабанихин С. И. Обратные и некорректные задачи. – Учебник: СНИ, 2008. – [Електронний ресурс]: http://www.twirpx.com/file/ 238358/ – Режим доступу: вільний.

94. Арсенин В.Я., Тихонов А.Н. Некорректные задачи / Математическая энциклопедия. – Сов. энциклопедия, 1982. – Т.3. – С.930-935. – [Електронний ресурс]: http://dic.academic.ru/dic.nsf/enc_mathematics/3375/Некорректные. – Режим доступу: вільний.

95. Відновлення та оптимізація інформації в системах прийняття рішень / Баранов В.Л., Браіловський М.М., Засядько А.А., Казакова Н.Ф., Хорошко В.О. // Підручник. – К.: Видн. ДУІКТ, 2009. – 134 с.

96. Верлань А.Ф., Сизиков В.С. Интегральные уравнения: методы, алгоритмы, программы. Справочное пособие. – К.: Наукова думка, 1986. – 544 с. – [Електронний ресурс]: http://www.twirpx.com/file/273092/ – Режим доступу: вільний.

97. Морозов В.А. Регулярные методы решения некорректно поставленных задач. – М.: Наука, 1987. – 240 с. – [Електронний ресурс]: http://www.srcc.msu.su/nivc/sci/books/morozov6. html – Режим доступу: вільний.

98. Морозов В.А. Об устойчивых методах решения систем линейных алгебраических уравнений // Вычислительные методы линейной алгебры. – Новосибирск: СО АН СССР, 1974.

99. Тихонов А.Н. О регуляризации некорректно поставленных задач // Доклады АН СССР. – №3, 1963. – С. 501-504. – [Електронний ресурс]: http://www.mathnet.ru/php/getFT.phtml?jrnid=zvmmf&paperid=7494&what=fullt&option_lang=rus – Режим доступу: вільний.

100. Бакут, П. А. Вопросы статистической теории радиолокации : монография / П. А. Бакут, И. А. Большаков [и др.]. – М. : Сов. радио, 1964. – 426 с.

101. Трис, В. Теория обнаружения оценок и модуляции : монография / Ван Трис Г. – М. : Сов. радио, 1972. – 744 с.

102. Гуткин, Л. С. Проблемы оптимизации радиосистем [Текст] / Л. С. Гуткин // Радиотехника. – М. : Радиотехника. – 1971. – №5. – С. 21-29.

103. Гуткин, Л. С. Оптимизация радиоэлектронных устройств по совокупности показателей качества : монография / Л. С. Гуткин. – М. : Сов. радио, 1974. – 368 с.

104. Скопа, А. А. Анализ влияния точности измерения параметров радиоканала на помехоустойчивость приема [Текст] / А. А. Скопа, Н. М. Билык // Наукові записки УНДІЗ. – К. : УНДІЗ. – 2007. – №1. – С. 79-85.

105. Скопа, О. О. Проектний аналіз оцінювання ступеня ризику при скороченні обсягу профілактичних вимірювань об’єктів інфомереж / О. О. Скопа, Н. Ф. Казакова // Вісник Львівського національного

аграрного університету: Агроінженерні дослідження. – Львів : ЛНАУ. – 2008. – №12. – Т.1. – С. 66-71.

106. Грабовський, О. В. Аналіз показників якості інформаційно-вимірювальних систем [Текст] / О. В. Грабовский // Вісник національного університету «ХПІ». – Харків : НТУ ХПІ. – 2013. – С. 59-66.

107. Грабовський, О. В. Організація вимірювання на мережах рухомого зв‘язку [Текст] / О. В. Грабовский // Вимірювальна та обчислювальна техніка в технологічних процесах : міжнар. наук. техн. конф., 2007 р. : тези допов. – Хмельницький, 2007. – С. 33.

108. Колесникова, Е. В. Методы оценки качества технических систем [Текст] / Е. В. Колесникова, Г. В. Кострова, И. В. Прокопович // Труды Одесского политехнического университета. – О. : ОНПУ. – 2007. – №1(27). – С. 128-130 : [Електронний ресурс] / Портал : ОНПУ. – Режим доступу \www/ URL: http://pratsi.opu.ua/app/ webroot/ articles/1312992391.pdf. – Заголовок з контейнера, доступ вільний, 30.10.2012.

109. Кириллов, В. И. Квалиметрия и системный анализ : навч. посібник / В. И. Кириллов. – Минск : Новое знание ; М. : ИНФРА-М, 2011. – 440 с. : ил. – (Высшее образование). – ISBN 978-985-475-353-9 (Новое знание) ; ISBN 978-5-16-004689-1 (ИНФРА-М).

110. Пегат, А. Нечеткое моделирование и управление / А. Пегат ; пер. с англ. – М. : БИНОМ. Лаборатория знаний, 2009. – 798 с. : ил. – (Адаптивные и интеллектуальные системы). – ISBN 978-5-94774-353-1 (русск.), ISBN 3-7908-1385-0 (англ.).

111. Адлер, Ю. П. Планирование эксперимента при поиске оптимальных условий : моногорафія / Ю. П. Адлер, Е. В. Маркова, Ю. В. Грановский. – М : Наука, 1976. – 269 с. – ISBN відсутній.

112. Федорченко, С. Г. Обобщенная функция полезности и ее приложения : монографія / С. Г. Федорченко, Ю. А. Долгов, А. В. Кирсанова [та ін.] / Під ред. С. Г. Федорченко. – Тирасполь : Приднестровский ун-т, 2011. – 196 с. – ISBN978-9975-4062-3-9.

113. Ногин, В. Д. Принятие решений в многокритериальной среде: количественный подход : монографія. – М. : ФИЗМАТЛИТ, 2002. – 144 с. – ISBN 5-9221-0274-5.

114. Батищев, Д. И. Оптимизация многоэкстремальных функций с помощью генетических алгоритмов / Д. И. Батищев, С. А. Исаев // Межвуз. сборник : Воронеж, ВГТУ. – 1997. – №3. – с. 4-17.

115. Кучерявый, А.Е. Качество обслуживания и качество восприятия. Рекомендации МСЭ-Т [Электронный ресурс] / Портал : ITU. – Режим доступа \www/ URL: : http://www.itu.int/en/ITU-D/Regulatory-

Market/.../Session3_Kucheryaviy.pdf. – Заголовок с конейнера, доступ свободный, 30.07.2013.

116. Y.1541 : Network performance objectives for IP-based services [Электронный ресурс] / Портал : ITU. – Режим доступа \www/ URL: http://www.itu.int/rec/T-REC-Y.1541/en. – Заголовок с экрана, доступ свободный, 29.07.2013.
117. СОУ 64.2-00017584-008 : 2010 «Телекомунікаційні мережі передачі даних загального користування. Система показників якості услуг з передачі даних та доступу до Інтернет. Загальні положення» [Електронний ресурс] / Портал : document.ua. – Режим доступу \www/ URL: http://document.ua/sou-64.2-00017584-008-2010-srrsdoc-srh3000531215. html. – Заголовок з екрану, доступ вільний, 29.07.2013.
118. СОУ 64.2-00017584-009:2010 «Телекомунікаційні мережі передачі даних загального користування. Телекомунікаційні послуги. Показники якості. Методи випробувань та оцінки» [Електронний ресурс] / Портал : document.ua. – Режим доступу \www/ URL: http://document. ua/sou-64.2-00017584-009-2010-srrsdoc-srh200053 4389.html. – Заголовок з екрану, доступ вільний, 29.07.2013.
119. Y.1291 : An architectural framework for support of Quality of Service in packet networks [Электронный ресурс] / Портал : ITU. – Режим доступа \www/ URL: http://www.itu.int/rec/T-REC-Y.1291/en. – Заголовок с конейнера, доступ свободный, 30.07.2013.

ДОДАТОК

Терміни та означення

Означення 1.1. *Теорія розпізнавання образів* – це розділ інформатики, що розвиває теоретичні основи і методи класифікації та ідентифікації предметів, явищ, процесів, сигналів, ситуацій і т. п. об'єктів, які характеризуються кінцевим набором деяких властивостей та ознак.

Означення 1.2 *Образ* – класифікаційне угруповання в системі класифікації, яка об'єднує (виділяє) певну групу об'єктів за певною ознакою.

Означення 1.3. *Розпізнавання* – це віднесення вихідних даних до певного класу за допомогою виділення істотних ознак, що характеризують ці дані, із загальної маси несуттєвих даних.

Означення 1.4. *Ідентифікація* – це присвоєння суб'єктам і об'єктам ідентифікатора і/або порівняння його з переліком визначених ідентифікаторів.

Слідуючи зі сказаного та враховуючи Означення 1.3 та 1.4, можна зробити висновок про те, що у тому розумінні, як це прийнято на сьогоднішній день у СЗІ, до *типових завдань аналізу зображень* можна віднести розпізнавання рукописних або друкованих знаків, дешифрування аеро- та космічних фотознімків, аналіз спостережуваних сцен, ангіографію та ін., а аналіз зображень у тому сенсі, як це поставлено у меті роботи, є окремою науковою проблемою.

Стосовно загальної класифікації по Т. Павлідісу, *синтез зображень* ототожнюється з машинною графікою, хоча останній термін в буквальному розумінні вже став архаїчним. В даний час на ЕОМ синтезуються аж ніяк не тільки «графічні» картини, а навпаки, синтез все більше претендує на створення повнокольорових реалістичних зображень за їх описами в необразотворчій формі. Але, в переважній більшості, сюди відносяться лише:

– системи імітації візуальної обстановки на тренажерах;

– системи геометричного моделювання в САПР;

– системи комп'ютерного кіномистецтва.

Інших задач синтезу, класифікацією по Т. Павлідісу не передбачається.

Приведемо відомі біометричні показники, які можуть використовуватися стосовно задачі ідентифікації особи абонента інформаційної або іншої мережі з обмеженим доступом.

Означення 1.5. *Розпізнавання особи* – це практичний додаток до теорії розпізнавання образів, в завдання якого входить автоматична локалізація особи на зображенні.

Означення 1.6. *Ідентифікація особи* – це практичний додаток до теорії функціонування систем захисту інформації, завданням якого є автоматичне присвоєння суб'єктам і об'єктам ідентифікатора на основі його кореляційної обробки з переліком визначених ідентифікаторів.

Означення 1.7. *Спостереженість* – властивість системи, що дозволяє фіксувати діяльність користувачів та процесів, використання пасивних об'єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії.

Означення 1.8. *Авторизація* – надання певній особі або групі осіб прав на виконання певних дій, а також процес перевірки (підтвердження) даних прав при спробі виконання цих дій.

Часто можна почути вираз, що особа «авторизована» для виконання даної операції. Це означає, що саме ця особа має право на таку дію. Як видно, це висловлювання в своїй історії має походження від англійського слова *authorization* – дозвіл, уповноваження. Таке поняття більше стосується банківських та інших платіжних систем. Його науковий смисл може бути виражений у означенні, яке тут приводиться з метою розрізнення далі використовуваних термінів та понять.

Означення 1.9. *Авторизація* – перевірка прав користувача на здійснення транзакцій, які проводяться в точці обслуговування, результатом якої є дозвіл або заборона операцій клієнта.

Згідно до діючих документів та нормативних вимог, авторизацію не слід плутати з аутентифікацією: *аутентифікація* – це лише процедура перевірки достовірності даних, наприклад, перевірки відповідності введеного користувачем пароля до облікового запису паролю в базі даних, або перевірка цифрового підпису листи по ключу шифрування, або перевірка контрольної суми файлу на відповідність заявленій автором цього файлу. Враховуючи сказане, приведемо відповідне визначення так, як це сформульовано у [22].

Означення 1.10. *Аутентифікація* – це процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора.

Означення 1.11. *Ідентифікатор* – ознака, яка служить для ідентифікації особи чи предмета, що розпізнається.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

ЗВІТ

про наукову діяльність

кафедри **ІНФОРМАЦІЙНИХ СИСТЕМ В ЕКОНОМІЦІ**

за 2013 рік

Одеса – 2013

АНОТОВАНИЙ ЗВІТ

I. Назва науково-дослідної роботи (НДР), номер державної реєстрації

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

Номер державної реєстрації 0112U007713;
Супровідний лист від 17 грудня 2012 року №01-17/2206

II. Характер НДР

- ☐ фундаментальне дослідження
- ⊕ прикладне дослідження
- ☐ прикладна розробка

III. Керівник науково-дослідної роботи (ПІБ, вчений ступінь, звання, посада, членство в НАНУ або в державних галузевих академіях наук)

***Скопа Олександр Олександрович**, докт. техн. наук, доцент*

IV. Виконавці: *штатні – 8, сумісники та ін. – 6*

доктори наук, професори 1
кандидати наук, доценти 6
в т.ч. здобувачі наукового ступеня докт. наук 2
ст. викладачі 4
в т.ч. здобувачі наукового ступеня канд. наук 2
викладачі 1
в т.ч. здобувачі наукового ступеня канд. наук 1
аспіранти 2
студенти 10

V. Строки виконання роботи

початок *січень, 2013*
закінчення *грудень, 2017*

VI. Обсяг фінансування

Роботи виконуються в рамках другої половини дня викладачами кафедри за рахунок бюджетних засобів

Код джерел фінансування	Загальний обсяг фінансування, тис. грн	у тому числі за роками				
		2013	2014	2015	2016	2017
7713	490,0	98,0	98,0	98,0	98,0	98,0

VII. Короткий зміст проекту НДР

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

Основні завдання для досягнення мети

Основними завданням для досягнення мети роботи є розробка та удосконалення методологій, методик, методів та засобів 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, 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 підприєствами 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 спіробітників підприємств та організацій сфери економіки, бізнесу та фінансів у галузі інформаційної та фінансово-економічної безпеки.*

VIII. Заплановані очікувані наукові результати

(відповідно до станів календарного плану НДР)

№ п/п	Зміст етапів роботи	Відповідальні за етапи	Термін виконання		Результати та впровадження
			початок	кінець	
1	2	3	4	5	6
1	Розробка та удосконалення методологій, методик, методів та засобів 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	д.т.н., доц. О.О. Скопа к.т.н., доц. Н.Ф. Казакова; к.е.н., доц. О.В. Орлик к.т.н., доц. Ю.В. Щербина к.е.н., ст. викл. О.І. Мацків ст. викл. О.Г. Єсіна ст. викл. А.Ю. Вакула ст. викл. О.О. Фразе-Фразенко викл. О.О. Йона	10.01.13	31.12.13	статті; доповіді на конференціях; тези та матеріали доповідей; розділи колективної монографії; навчальні матеріали

2	Розробка та удосконалення методологій, методик, методів та засобів 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, у тому числі: конфіденційність та захист даних; забезпечення виконання стандартів та нормативних вимог підприєствами та організаціями; управління загрозами та уразливостями	д.т.н., доц. О.О. Скопа к.т.н., доц. Н.Ф. Казакова; к.е.н., доц. О.В. Орлик к.т.н., доц. Ю.В. Щербина к.е.н., ст. викл. О.І. Мацків ст. викл. О.Г. Єсіна ст. викл. А.Ю. Вакула ст. викл. О.О. Фразе-Фразенко викл. О.О. Йона	01.01.14	31.12.14	статті; доповіді на конференціях; тези та матеріали доповідей; розділи колективної монографії; навчальні матеріали
3	Розробка та удосконалення методологій, методик, методів та засобів 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, у тому числі: управління загрозами та уразливостями; забезпечення фізичної безпеки; тестування на проникнення у системи захисту від несанкціонованого доступу; удосконалення архітектури інформаційної безпеки	д.т.н., доц. О.О. Скопа к.т.н., доц. Н.Ф. Казакова; к.е.н., доц. О.В. Орлик к.т.н., доц. Ю.В. Щербина к.е.н., ст. викл. О.І. Мацків ст. викл. О.Г. Єсіна ст. викл. А.Ю. Вакула ст. викл. О.О. Фразе-Фразенко викл. О.О. Йона	01.01.15	31.12.15	статті; доповіді на конференціях; тези та матеріали доповідей; розділи колективної монографії; навчальні матеріали

4	Розробка та удосконалення методологій, методик, методів та засобів 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, у тому числі: 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	д.т.н., доц. О.О. Скопа к.т.н., доц. Н.Ф. Казакова; к.е.н., доц. О.В. Орлик к.т.н., доц. Ю.В. Щербина к.е.н., ст. викл. О.І. Мацків ст. викл. О.Г. Єсіна ст. викл. А.Ю. Вакула ст. викл. О.О. Фразе-Фразенко викл. О.О. Йона	01.01.16	31.12.16	статті; доповіді на конференціях; тези та матеріали доповідей; розділи колективної монографії; навчальні матеріали

5	Розробка та удосконалення методологій, методик, методів та засобів 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, у тому числі: питання інформаційної безпеки у галузі поінформованості та навчання співробітників; питання підготовки кадрів та підвищення кваліфікації спіробітників підприємств та організацій сфери економіки, бізнесу та фінансів у галузі інформаційної та фінансово - економічної безпеки	д.т.н., доц. О.О. Скопа к.т.н., доц. Н.Ф. Казакова; к.е.н., доц. О.В. Орлик к.т.н., доц. Ю.В. Щербина к.е.н., ст. викл. О.І. Мацків ст. викл. О.Г. Єсіна ст. викл. А.Ю. Вакула ст. викл. О.О. Фразе-Фразенко викл. О.О. Йона	01.01.17	31.12.17	статті; доповіді на конференціях; тези та матеріали доповідей; колективна монографія; навчальні матеріали

IX. Перелік найголовніших завдань

Розробка та удосконалення методологій, методик, методів та засобів для підприємств та організацій сфери економіки, бізнесу та фінансів у галузі інформаційної та фінансово-економічної безпеки щодо:

- *управління ідентифікаційною інформацією і доступом;*
- *управління інформаційною та фінансово-економічною безпекою підприємств;*
- *засобів захисту даних;*
- *забезпечення виконання стандартів та нормативних вимог підприєствами та організаціями;*
- *управління загрозами та уразливостями;*
- *питання інформаційної безпеки у галузі поінформованості та навчання співробітників;*
- *питання підготовки кадрів та підвищення кваліфікації спіробітників.*

X. Отримані найважливіші наукові результати (1 етап НДР)

Розділ 1 УПРАВЛІННЯ ІДЕНТИФІКАЦІЙНОЮ ІНФОРМАЦІЄЮ І ДОСТУПОМ

Встановлено, що централізоване управління ідентифікаційною інформацією, корпоративною політикою безпеки та захистом корпоративних мереж і міжмережевих взаємодій для підприємств та організацій сфери економіки, бізнесу та фінансів, а також для інших зацікавлених фізичних та юридичних осіб – це ті три основних компоненти на які спирається безпека будь-якого бізнесу.

Показано, що у зв'язку з постійно зростаючою кількістю корпоративних додатків, що вимагають розмежування прав доступу, розгортання централізованого управління ідентифікаційною інформацією забезпечує відчутне зростання продуктивності підприємств, зменшуючи при цьому витрати, пов'язані з управлінням так званим «ідентифікаційним хаосом» різнорідних додатків. Відповідно, для вирішення окремих завдань стосовно зазначеного, отримані рішення, призначені для інтеграції розрізнених систем ідентифікації користувачів в складі гетерогенних систем на базі єдиного корпоративного каталогу та побудови централізованої системи управління правами доступу користувачів на основі принципів рольового доступу.

Отримані рішення дозволяють в майбутньому здійснювати такі функції:

– проводити аутентифікацію та авторизацію користувачів гетерогенних систем на основі біометричних пристроїв;

– виконувати централізоване адміністрування процесу реєстрації облікових записів користувачів, у тому числі – самообслуговування користувачем його персональної інформації;

– централізоване управління правами доступу користувачів на основі їх бізнес- ролей;

– централізований аудит привілеїв користувачів, включаючи привілеї груп, в які він входить, ролей, які йому призначені, і переліку доступних йому ресурсів;

– делегування повноважень адміністраторам окремих додатків, груп, територіальних об'єднань і т. д.

Науковою новизною отриманих результатів у сенсі управління ідентифікаційною інформацією і доступом є упорядкування і централізація процедури доступу до додатків і мережевих сервісів на основі актуальних ідентифікаційних даних користувачів.

Практичне значення результатів полягає у зниженні адміністративних витрат на розгортання, інтеграцію і підтримку механізмів управління доступом користувачів до різних корпоративних додатків і платформ, а також істотне зростання рівня захищеності інформаційних ресурсів підприємств та організацій сфери економіки, бізнесу та фінансів за рахунок усунення «ідентифікаційного хаосу» використовуваних різнорідних додатків і платформ.

Отримані результати, у відповідності до вище зазначених наукової новизни та практичного значення, відповідають рівню аналогічних розробок, отриманих науковими приацівниками та вченими світового рівня. Їх достовірність, точність та коректність підтверджені достатньою кількість наукових публікацій у виданнях за переліками ВАК України та у виданнях, що входять до міжнародних наукометричних баз даних.

Розділ 2 УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА ФІНАНСОВО-ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВ

Встановлено, що до показників економічної безпеки відносяться наступні:

– показник економічного зростання: динаміка і структура національного виробництва і доходу

– показники обсягів та темпів промислового виробництва;

– галузева структура господарства та динаміка окремих галузей, капіталовкладення та ін.;

– показники якості життя: ВВП на душу населення, рівень диференціації доходів, забезпеченість основних груп населення матеріальними благами і послугами, працездатність населення, стан навколишнього середовища і т.д.

Показано, що вище зазначені показники характеризують:

– природно-ресурсний, виробничий, науково-технічний потенціал країни;

– динамічність та адаптивність господарського механізму, а також його залежність від зовнішніх факторів: рівень інфляції, дефіцит консолідованого бюджету, дію зовнішньоекономічних чинників, стабільність національної валюти, внутрішню і зовнішню заборгованість.

Визначено, що економічна безпека – це здатність економіки забезпечувати ефективне задоволення суспільних потреб на національному і міжнародному рівнях, тобто, економічна безпека являє собою сукупність внутрішніх і зовнішніх умов, що сприяють ефективному динамічному зростанню національної економіки, її здатності задовольняти потреби суспільства, держави, індивіда, забезпечувати конкурентноздатність на зовнішніх і внутрішніх ринках, що гарантує від різного роду загроз і втрат.

Науковою новизною дослідження є встановлення того факту, що економічна безпека для підприємств та організацій сфери економіки, бізнесу та фінансів повинна забезпечуватися, насамперед, ефективністю самої економіки країни, тобто, поряд із захисними заходами, здійснюваними державою, вона повинна захищати сама себе на основі високої продуктивності праці, якості продукції і т.д. Т.ч., забезпечення економічної безпеки не є прерогативою якого-небудь одного державного відомства, служби і, відповідно, вона повинна підтримуватися всією системою державних органів, всіма ланками і структурами економіки.

Практичним значенням отриманих результатів є те, що з’явилася можливість встановити порогові рівні зниження безпеки та охарактеризувати їх системою показників загальногосподарського і соціально-економічного значення, які, зокрема, відображають:

– гранично допустимий рівень зниження економічної активності, обсягів виробництва, інвестування та фінансування, за межами якого неможливо самостійне економічний розвиток підприємств та організацій сфери економіки, бізнесу та фінансів на технічно сучасному, конкурентоспроможному базисі

– підтримання оборонного, науково-технічного, інноваційного, інвестиційного та освітнього потенціалу.

Отримані результати, у відповідності до вище зазначених наукової новизни та практичного значення, відповідають рівню аналогічних розробок, отриманих науковими приацівниками та вченими світового рівня. Їх достовірність, точність та коректність підтверджені достатньою кількість наукових публікацій у виданнях за переліками ВАК України та у виданнях, що входять до міжнародних наукометричних баз даних.

Розділ 3 КОНФІДЕНЦІЙНІСТЬ ТА ЗАХИСТ ДАНИХ

Встановлено, що одним з найбільш поширених в науці інформаційного права є уявлення про те, що при отриманні конфіденційної інформації відповідний режим таємниці трансформується з одного режиму в інший. При цьому відмічено, що відомості про діяльність будь-яких господарюючих суб'єктів та фізичних та юридичних осіб в цілому, які можуть бути предметом комерційної таємниці, функціонують в режимі, наприклад, банківської таємниці. Відповідно комерційна, професійна, банківська таємниця, персональні дані при наданні їх в органи державного управління не припиняють своє функціонування, а складають службові відомості, доступ до яких обмежений органами державної влади відповідно до діючого законодавства, так як до органів виконавчої влади надається не режим, а інформація.

Показано, що всередині підприємств та організацій сфери економіки, бізнесу та фінансів можуть функціонувати відомості, що становлять комерційну таємницю, персональні дані, різновиди професійної таємниці, щодо яких володар повинен забезпечити конфіденційність.

Відповідно до вище зазначеного, **визначено** питання, які можуть бути предметом подальшого вивчення та дослідження, а саме:

– які заходи для забезпечення конфіденційності повинні розробляти підприємства та організації сфери економіки, бізнесу та фінансів;

– чи повинні організації та підприємства в обов'язковому порядку встановлювати режим комерційної таємниці;

– забезпечення режиму захисту персональних даних;

– забезпечення режиму професійної таємниці.

Науковою новизною дослідження є:

– встановлення того факту, що режим конфіденційності інформації у сфері економіки, бізнесу та фінансів є предметом правового регулювання, яке представляє особливий порядок, встановлений державою у вигляді правових норм і забезпечений силою державного примусу за допомогою застосування будь-яких

дій з інформацією конфіденційного характеру, включаючи збір, систематизацію, накопичення, зберігання, уточнення, оновлення, зміни, використання, розповсюдження (у тому числі передачу), блокування, знищення;

– для забезпечення конфіденційності однієї і тієї ж інформації існує можливість встановлювати різні режими, які, втім, можуть привести до виникнення конфліктів інтересів суб'єктів таємниць. Для виключення конфліктів при здійсненні інформаційного обміну показана доцільність закріплення в нормативних актах поняття «режим конфіденційності інформації», який дозволив би встановити єдині правила та вимоги до забезпечення безпеки інформації як в органах державної влади, так і господарюючих суб'єктів.

Практичним значенням отриманих результатів є те, що:

– на основі оцінки ризиків можливе виявлення загроз активам, оцінка уразливості відповідних активів і ймовірності виникнення загроз, а також оцінка можливих наслідків;

– використання законодавчих вимог для забезпечення узгодженості, цілеспрямованості, планомірності діяльності щодо забезпечення інформаційної безпеки веде до підвищення рівня захищеності будь-якого підприємства сфери економіки, бізнесу та фінансів;

– з'явилася можливість визначення адекватності заходів захисту з урахуванням принципу оптимальності витрат на захист інформації.

Отримані результати, у відповідності до вище зазначених наукової новизни та практичного значення, відповідають рівню аналогічних розробок, отриманих науковими приацівниками та вченими світового рівня. Їх достовірність, точність та коректність підтверджені достатньою кількість наукових публікацій у виданнях за переліками ВАК України та у виданнях, що входять до міжнародних наукометричних баз даних. За результатами досліджень опубліковану 1 монографію та отримано 1 патент на винахід.

XI. Отримана науково-методична, або науково-технічна продукція (1 етап НДР)

(кількість захищених дисертацій, опублікованих монографій, підручників, навчальних посібників, у т.ч. з грифом МОНУ, статей, тез, доповідей на конференціях, патентів)

Опубліковано монографій _____ 1;
Отримано патентів _____ 1;
Опубліковано статей _____ ;
Опубліковано тез, доповідей на конференціях_____ .

XII. Практична цінність результатів та продукції (1 етап НДР)

Основний зміст розроблених технологій, засобів та методик практичного спрямування

Огляд та аналіз поточного стану технологій ідентифікації та управління доступом, а також перспективи використання їх у сучасних системах захисту інфо-

рмації на підприємствах та організаціях сфери економіки, бізнесу та фінансів, показав наступне:

1) Задача аналізу, переробки та відображення візуальної інформації, як завдання щодо розвитку та створення пристроїв ідентифікації особи абонента з використанням біометричних даних в цілях захисту інформації від несанкціонованого використання або навмисного спотворення, відноситься до проблем, які вирішуються у рамках теорії розпізнавання образів.

2) Визначено місце завдання ідентифікації особи абонента на основі використання його біометричних даних у загальній схемі функціонування технологічної системи, яка використовує систему захисту інформації (СЗІ) та технології прогнозування стану при виникненні в ній інцидентів.

3) Виділені основні поняття теорії розпізнавання образів, які можуть бути використані при розробці положень щодо створення пристроїв ідентифікації особи абонента з використанням біометричних даних в цілях захисту інформації.

4) Показано, що не зважаючи на загальну негативну оцінку сучасного стану біометричних систем ідентифікації особистості, спостерігається тенденція до розвитку досліджень та розробок в області біометрії. При цьому однією з основних тенденцій є поступовий перенос пріоритетів з контактних на безконтактні методи біометричного розпізнавання.

5) Виділено три групи специфічних проблем, які не мають адекватного роз'язку у сенсі створення біометричних систем нового покоління. На основі їх аналізу показана необхідність комплексування результатів біометричного розпізнавання, отриманих від різних джерел інформації.

6) Виділено 2 напрямки, які існують у практиці розпізнавання образів. Базуючись на них, стосовно задач, які вирішуються в НДР, обрано той, що розвиває теоретичні принципи та практичні методи побудови пристроїв, призначених для вирішення окремих завдань СЗІ в прикладних цілях.

7) Виділено 4 напрямки, які існують у практиці досліджень проблеми розпізнавання осіб. З врахуванням п. 6, обрано напрямок, який є комплексним та базується на дослідженні інформаційно-процесуальних моделей зі створенням комп'ютерних моделей розпізнавання.

8) Виконано формальну постановку завдання до НДР у сенсі змісту розділу 1 щодо управління ідентифікаційною інформацією і доступом, яке поягає в удосконаленні та підвищенні ефективності методів та технологій, які забезпечують процедуру аутентифікації у СЗІ на основі використання біометричних технологій для підприємств та організацій сфери економіки, бізнесу та фінансів.

9) Розроблено загальну схему дослідження, якою передбачено використання логічних розмірковувань та адекватиних математичних доказів. Схема відповідає класичній постановці задачі розпізнавання образів у системах забезпечення спостереженості.

10) Проведено огляд та вибір інформативних ознак зображень для розв'язку задачі біометричної ідентифікації особи, а також вибір предмета та технології розпізнавання. Як результат показано, що розв'язком проблеми вибору інформативних ознак для систем біометричної ідентифікації, може бути використання системи ознак, яка базується на побудові одномірних гістограм. При цьому, з посиланням на матеріали наступних розділів, виділена необхідність попередньої обробки зображень з метою поліпшення якості розпізнавання та його ймовірності.

Визначення та обґрунтування
патенто- і ліцензійно спроможних результатів

На поточному етапі досліджень патенто- і ліцензійно спроможних результатів з удосконалення та підвищення ефективності методів та технологій, які забезпечують процедуру аутентифікації у СЗІ на основі використання біометричних технологій не отримано.

Нові конкурентоспроможні товари та послуги,
які будуть або вже створені на базі результатів роботи

Нові конкурентоспроможні товари та послуги для підприємств та організацій сфери економіки, бізнесу та фінансів, на базі результатів роботи будуть визначатися та встановлюватися на останньому етапі НДР.

Інвестиційна привабливість, обґрунтований економічний,
соціальний та інший ефект результатів роботи

Інвестиційна привабливість, обґрунтований економічний, соціальний та інший ефект результатів досліджень для підприємств та організацій сфери економіки, бізнесу та фінансів, будуть визначатися та встановлюватися на останньому етапі НДР.

Підприємства, організації, установи, заклади, що впроваджують результати, шляхи просування на ринок

Підприємства, організації, установи та заклади сфери економіки, бізнесу та фінансів, що впроваджують результати, а також шляхи їх просування на ринок, будуть визначатися та встановлюватися на третьому та четвертому етапах НДР.

XIII. Використання результатів у навчальному процесі (1 етап НДР)
Нові спеціальності, спеціалізації, курси лекцій або їх розподіли, практичні та лабораторні роботи, які (будуть) започатковані на основі результатів цього наукового дослідження в навчальному процесі

На основі результатів наукових досліджень, проведених на 1 етапі НДР, стосовно розділу «Управління ідентифікаційною інформацією і доступом», для навчального процесу кафедри:

– 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 у виданій монографії за темою дослідження, можуть бути використані при підготовці бакалаврів спеціальності 8.18010014 «Управління фінансово-економічною безпекою» кваліфікації «Професіонал з фінансово-економічної безпеки» та «Аналітик з питань фінансово-економічної безпеки».

Перелік докторських і кандидатських дисертацій, що захищені та підготовлені на базі науково-дослідної роботи за час її виконання
(найменування дисертації, докторська чи кандидатська, автор, науковий керівник або консультант, для захищених – дата захисту)

На базі науково-дослідної роботи виконуються та готуються до захисту:

1) докторські дисертації

– «Розвиток теорії та удосконалення принципів багаторівневого захисту інфор-мації у недовірених системах» (ДСК), автор канд. техн. наук, доц. Казакова Н.Ф., науковий консультант докт. техн. наук, доц. Скопа О.О.;

– «Теорія вирішення завдань забезпечення фінансово-економічної безпеки на основі системного аналізу і нечіткого когнітивного моделювання» (ДСК), автор канд. екон. наук, доц. Орлик О.В., науковий консультант докт. техн. наук, доц. Скопа О.О.

2) кандидатські дисертації

– «Підвищення ефективності методів забезпечення превентивної безпеки у системах з обмеженим доступом» (ДСК), автор ст. викл. Фразе-Фразенко О.О., науковий керівник канд. техн. наук, доц. Казакова Н.Ф.;

– «Удосконалення методів забезпечення захисту персональних даних у системах Інтернет-банкінгу» (орієнтовна тема), автор ст. викл. Єсіна О.Г., науковий керівник канд. техн. наук, доц. Казакова Н.Ф.;

– «Удосконалення технологій інтерпретації ризик-орієнтованих оцінок інформаційної безпеки» (орієнтовна тема), автор викл. Йона О.О., науковий керівник докт. техн. наук, доц. Скопа О.О.

Кількість курсових, дипломних та інших робіт, що захищені на базі зазначеної наукової роботи за час її виконання

Виконання курсових, дипломних та інших робіт на базі наукової роботи не передбачається навчальними планами напрямів та спеціальностей у зв‘язку з тим, що кафедра не є випускною.

Використання результатів у науковій роботі, науково-технічній та інноваційній діяльності студентів, в інших закладах освіти

Результати, отримані при виконанні НДР, використовуються у науковій роботі, науково-технічній та інноваційній діяльності студентів при проведенні студентських олімпіад та конференцій з документуванням їх у протоколах засідання секцій.

XIV. Основні висновки

При виконанні 1-го етапу НДР розроблені та удосконалені окремі методології, 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: з управлінням ідентифікаційною інформацією і доступом; управлінням інформаційною та фінансово-економічною безпекою підприємств; зі збереженням конфіденційності та захистом даних.

XV. Рішення факультету від «___» _____201__р. (протокол № ____) про закінчення етапу роботи та пропозиції щодо її впровадження, продовження тощо.

Науковий керівник **О.О. Скопа**

Декан факультету **П.І. Островський**