ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
Міністерство освіти і науки України

Кваліфікаційна наукова робота

На правах рукопису

БРЖЕВСЬКА ЗОРЕСЛАВА МИХАЙЛІВНА

УДК 004.056

ДИСЕРТАЦІЯ

МЕТОДИКА ОЦІНКИ ДОСТОВІРНОСТІ ІНФОРМАЦІЇ В УМОВАХ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА

Спеціальність 125 Кібербезпека

Подається на здобуття наукого ступення

Доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ З.М. Бржевська

Науковий керівник:

ГАЙДУР Галина Іванівна

Доктор технічних наук, професор

Київ 2021

АНОТАЦІЯ

Бржевська З.М. Методика оцінки достовірності інформації в умовах інформаційного протиборства. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 125 Кібербезпека. – Державний університет телекомунікацій, м. Київ, 2021.

Виходячи з реалій сьогодення ефективність функціонування будь-якої організації, підприємства та держави залежить не тільки від надійності функціонування інформаційно - телекомунікаційних систем, а й у значній мірі від захищеності їх інформаційних ресурсів та інформації взагалі [1]. Однією з проблем, яка стримує впровадження ефективних систем захисту інформаційних ресурсів організації чи держави, є проблема створення достовірної класифікації атак та механізмів «фільтрування» інформації, яка проходить від першоджерела до споживача. Зважаючи на це, підвищення ефективності виявлення атак на інформаційні ресурси, залишається актуальним завданням. Систематизація знань про атаки допомагає розробці заходів і систем захисту від них. Тому фахівці в області інформаційної безпеки не припиняють спроб побудови різних класифікаційних схем, які в тій чи іншій мірі сприяють розумінню процесів, що ведуть до проникнення в системи, і допомагають розробляти заходи захисту і реалізовувати системи захисту.

Процес передачі інформації від офіційного джерела чи з “місця події” до кінцевого споживача є достатньо складним і тривалим. Під час свого просування інформація циркулює в інформаційному просторі і перебуває під впливом різних груп впливу, які переслідують власні інтереси. Отже, дуже часто кінцевий користувач отримує упереджену, необ’єктивну інформацію, метою якої є вчинення певного впливу на його поведінку.

Ситуація ускладнюється у випадку обмеженості джерел інформації, їх суб'єктивності та упередженості, які складають сутність інформаційного протиборства, коли протидіючі сторони намагаються будь-що чинити інформаційний тиск як на джерела інформації так і на увесь процес її розповсюдження. Для забезпечення нормального функціонування, прийняття адекватних рішень завданням кінцевого користувача є одержання об'єктивної своєчасної інформації, для чого на передній план виступають питання оцінювання її достовірності.

Питанням інформаційної взаємодії та оцінювання достовірності інформації присвячено значну кількість робіт вітчизняних та іноземних науковців. Так, у роботах Д.А. Губанова, Д.А. Новікова, А.Г. Чхартишвілі розглядається широке коло питань взаємодії користувачів у соціальних мережах. Роботи Г.Г. Почепцова, О.К. Юдіна, Р.В. Грищука, К.В Молодецької, В.П. Городнова, А.П. Верьовченка, В.В. Горчакова присвячені теоретичним та практичним аспектам інформаційного протиборства. Публікації М.Ю. Монахова, Д.А. Полянського, І.І. Семенова, К.Г. Абрамова, І.Р. Конєєва, А.В. Беляєва, Г.І. Гайдур, Н.М. Довженко та ін. присвячені оцінюванню достовірності інформації та її джерел.

Разом з тим, незважаючи на значну кількість публікацій щодо вирішення різноманітних аспектів оцінювання достовірності інформації на сьогоднішній день залишається невирішеною проблема комплексного оцінювання достовірності з урахуванням можливого інформаційного впливу на ресурси та канали передачі інформації.

Основне протиріччя, яке лежить в основі наукового дослідження полягає, з одного боку в тому, що інформація, яка добувається, передається та зберігається, не завжди може бути представлена у вигляді даних чи відомостей на машинних носіях у стандартизованому чи формалізованому вигляді, а, відтак потребує особливих підходів щодо її захисту від спотворення. З іншого боку, вплив інформаційного протиборства, який також є інформаційним,

також не може бути представленим методами формальних теорій та числень, що унеможливлює його оцінювання під час оцінки достовірності інформації.

Отже, вирішенню підлягає актуальне наукове завдання щодо розроблення методики оцінювання достовірності інформації в умовах інформаційного протиборства для захисту інформаційних ресурсів організації та забезпечення інформаційної безпеки користувачів.

Дисертаційна робота виконана відповідно до положень Законів України “Про інформацію”, “Про концепцію національної програми інформатизації”, “Про телебачення і радіомовлення”, “Про телекомунікації”; Доктрини інформаційної безпеки України, затвердженої Указом Президента України від 25.02.2017 р. № 47/2017; Стратегії національної безпеки України, затвердженої Указом Президента України від 14.09.2020 № 392/2020, та плану наукової та науково-технічної діяльності Державного університету телекомунікацій у рамках науково-дослідних робіт: “Розробка методів та засобів підвищення живучості інформаційно-комунікаційних систем в умовах впливу кібернетичних атак”, шифр «Живучість К14» (№ ДР 0114U000391) де автором проведено аналіз факторів впливу інформаційного протиборства на інформаційні ресурси організації та інформаційно-телекомунікаційні системи; “Конкурентна розвідка як складова забезпечення інформаційної безпеки підприємства”, шифр “CompInt”, де автором запропоновано модель процесу управління достовірністю інформації та методику оцінки достовірності інформації в умовах інформаційного протиборства.

Мета дисертаційної роботи полягає полягає у підвищенні достовірності інформації, яка передається від першоджерела до користувача в умовах інформаційного протиборства.

Наукова новизна одержаних положень і результатів полягає в тому, що:

Удосконалено математичну модель інформаційного впливу, яка базується на системі диференційних рівнянь, що описують зміну кількості прихильників інформаційних повідомлень у залежності від індивідуальних

особливостей соціальних груп та, на відміну від існуючих, додатково враховує можливість забування та особливості засвоєння інформації окремими індивідами групи. Такий підхід дозволяє моделювати вплив на інформацію у процесі її проходження через різні засоби передачі та відтворювати процеси інформаційного протиборства, при проходженні повідомлень від першоджерела до кінцевого користувача;

Вперше розроблено модель процесу управління достовірністю інформації в умовах інформаційного протиборства, яка базується на моделі скінченного автомата із заданим кінцевим станом достовірності інформаційних повідомлень при відомому початковому стані інформаційних ресурсів і наборові допустимих дій. Такий підхід дає можливість реалізувати багатокрокову перевірку повідомлень з поступовим підвищенням показників достовірності у залежності від характеру повідомлень та ступеня впливу на їх зміст;

Удосконалено методику оцінки достовірності інформації в умовах інформаційного протиборства, яка базується на методі експертного оцінювання та, на відміну від існуючих, додатково враховує частоту виникнення факторів інформаційного протиборства та ймовірність спроб порушення достовірності інформації. Така методика дозволяє визначати кількісні та якісні показники достовірності інформації в інформаційному потоці в умовах впливів, які можуть описуватися як чіткими так і нечіткими змінними;

Вперше розроблено методику оцінки ризиків порушення достовірності інформації, яка передбачає встановлення залежності можливого збитку організації через порушення достовірності вхідної інформації від ступеня впливу конкретного фактора інформаційного протиборства на окремий інформаційний ресурс. Такий підхід дозволяє визначати найбільш доцільні заходи щодо забезпечення достовірності інформації, яка надається такими ресурсами кінцевим споживачам.

Нові наукові результати, одержані у роботі, у сукупності складають підґрунтя для створення системи захисту інформації на підприємстві чи організації в умовах інформаційного протиборства.

У роботі наведено комплекс алгоритмів перевірки достовірності інформації, які дозволяють сформувати систему управління інформаційним захистом підприємства на основі реалізації процедур управління достовірністю інформації.

Результати математичного моделювання та проведення практичного експерименту щодо створення системи забезпечення достовірності інформації у типовій організації дали можливість оцінити ефективність впровадження одержаних наукових результатів стосовно підвищення достовірності ресурсів за рахунок: підвищення адекватності моделей подання даних на 9–11%; підвищення якості організації інформаційного обміну на 6–8%; підвищення якості процедур контролю інформаційних ресурсів на 15–17%; підвищення кваліфікації персоналу на 17–19%.

У роботі запропоновано рекомендації щодо удосконалення політик безпеки для організацій різних форм власності, які функціонують в умовах інформаційного протиборства з боку конкурентів та недоброзичливців.

Результати досліджень прийняті до впровадження в ТОВ «ІТ Спеціаліст» (акт від 09.12.2020 р.), в ТОВ «Євротелеком» (акт від 07.12.2020 р.).

Ключові слова: достовірність інформації, інформаційні ресурси, інформаційний вплив, інформаційне протиборство, прихильник, інформаційний простір, суспільство, користувач, моделі, взаємодія, репутація, довіра, загрози.

ANOTATION

Zoreslava M. Brzhevska Method for assessing the reliability of the information in terms of information confrontation. – Qualifying scientific work on the rights of the manuscript.

The thesis on completion of a scientific degree of the Philosophy Doctor on a specialty 125 Cybersecurity. – State University of Telecommunications, Kyiv, 2021.

Based on today's realities, the effectiveness of any organization, enterprise, and state depends not only on the reliability of information and telecommunications systems but also largely on the security of their information resources and information in general [1]. One of the problems that hinder the implementation of effective systems of protection of information resources of the organization or the state is the problem of creating a reliable classification of attacks and mechanisms of "filtering" information that passes from the source to the consumer. In view of this, improving the effectiveness of detecting attacks on information resources remains an urgent task. Systematization of knowledge about attacks helps to develop measures and systems of protection against them. Therefore, information security experts do not stop trying to build different classification schemes, which to some extent contribute to the understanding of the processes leading to the penetration of systems, and help to develop protection measures and implement protection systems.

The process of transferring information from an official source or from the "scene" to the final consumer is quite complex and lengthy. During its promotion, information circulates in the information space and is influenced by various groups of influence that pursue their own interests. Thus, very often the end-user receives biased, biased information, the purpose of which is to exert a certain influence on his behavior.

The situation is complicated by the limited data sources, their subjectivity, and bias, which are the essence of information conflict when the opposing parties try to put any intelligence pressure on the data sources and the whole process of its

dissemination. To ensure the proper functioning, making adequate decisions, the task of the end-user is to obtain objective and timely information, for which the issues of assessing its reliability come to the fore.

A significant number of works by domestic and foreign scientists are devoted to the issues of information interaction and assessment of information reliability. Thus, in the works of D.A. Hubanov, D.A. Novikov, A.G Chkhartishvili addresses a wide range of issues of user interaction in social networks. Works by G.G. Pocheptsova, O.K. Yudin, R.V. Gryshchuk, K.V. Molodetska, V.P. Horodnov, A.P. Veryovchenko, V.V. Gorchakov are devoted to theoretical and practical aspects of information confrontation. Publications of M.Yu. Monakhov, D.A. Polyanskyi, I.I. Semenov, K.H. Abramov, I.R. Koneev, A.V. Belyaev, H.I. Haidur, N.M. Dovzhenko and others. devoted to assessing the accuracy of the information and its sources.

However, despite the significant number of publications on various aspects of assessing the reliability of the information, the problem of this assessment remains unresolved given the possible impact of information on resources and channels of information transmission.

The main contradiction underlying scientific research is, on the one hand, that information that is extracted, transmitted, and stored cannot always be presented in the form of data or information on machine media in a standardized or formalized form, and therefore requires special approaches to its protection against distortion. On the other hand, the influence of information confrontation, which is also informational, also cannot be represented by the methods of formal theories and calculations, which makes it impossible to assess it when assessing the reliability of the information.

Thus, the urgent scientific task of developing a methodology for assessing the reliability of the information in the context of information conflict to protect the information resources of the organization and ensure the information security of users is to be solved.

The dissertation was performed in accordance with the provisions of the Laws of Ukraine “On Information”, “On the Concept of the National Informatization Program”, “On Television and Radio Broadcasting”, “On Telecommunications”; Doctrines of information security of Ukraine, approved by the Decree of the President of Ukraine of Feb 25, 2017 № 47/2017; National Security Strategy of Ukraine, approved by the Decree of the President of Ukraine dated Sep 14, 2020 № 392/2020, and the plan of scientific and scientific-technical activities of the State University of Telecommunications in the framework of research: “Development of methods and means to increase the survivability of information and communication systems cyber-attacks ”, code“ Survival K14 ”(№ DR 0114U000391) where the author analyzes the factors of influence of information confrontation on the information resources of the organization and information and telecommunication systems; "Competitive intelligence as a component of information security of the enterprise", code "CompInt", where the author proposed a model of the process of information reliability management and methods of assessing the reliability of information in the context of information conflict.

The purpose of the thesis is to increase the reliability of information transmitted from the original source to the user in terms of information confrontation.

The scientific novelty of the obtained provisions and results is:

Improved mathematical model of information impact, which is based on a system of differential equations that describe the change in the number of supporters of information messages depending on individual characteristics of social groups and, unlike existing ones, additionally takes into account the possibility of forgetting and assimilation of information by individuals. This approach allows modeling the impact on the information in the process of its passage through various means of transmission and reproducing the processes of information confrontation in the passage of messages from the source to the end-user;

For the first time, a model of the information reliability management process in the conditions of information confrontation is developed, which is based on the finite state machine model with a given final state of information messages reliability at a known initial state of information resources and a set of valid actions. This approach makes it possible to implement a multi-step verification of messages with a gradual increase in reliability, depending on the nature of the messages and the degree of influence on their content;

Improved methodology for assessing the reliability of the information in the context of information confrontation, which is based on methods of expert evaluation and as existing ones decrease, additional study of the frequency of factors of information confrontation and reliability of attempts to violate the reliability of the information. This technique allows determining the quantitative and qualitative indicators of the reliability of the information in the flow under the influence, which can be described as clear and indistinct changes;

For the first time, a method of assessing the risks of breach of information is described, which provides for the dependence of possible damage to the organization due to breach of input information on the degree of influence of a particular factor of information confrontation on a particular information resource. This approach allows determining the most appropriate measures to ensure the reliability of the information provided by such resources to end-users.

The new scientific results obtained in the work, together, form the basis for the creation of a system of information protection at the enterprise or organization in the conditions of information conflict.

The paper presents a set of algorithms for verifying the accuracy of the information, which allow to formation of a management system for information protection of the enterprise based on the implementation of procedures for managing the reliability of the information.

The results of mathematical modeling and conducting a practical experiment to create a system for ensuring the reliability of information in a typical organization

made it possible to assess the effectiveness of the implementation of scientific results to increase the reliability of resources by: increasing the adequacy of data models by 9–11%; improving the quality of information exchange by 6–8%; improving the quality of control procedures for information resources by 15-17%; staff training by 17-19%.

The paper proposes recommendations for improving security policies for organizations of various forms of ownership, which operate in conditions of information confrontation by competitors and enemies.

The research results were accepted for implementation in LLC "IT Specialist" (the act from Dec 09, 2020), in LLC "Eurotelecom" (the act from Dec 07, 2020).

Keywords: reliability of the information, information resources, information influence, information confrontation, supporter, information space, society, user, models, interaction, reputation, trust, threats.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Наукові праці, у яких опубліковані основні наукові результати дисертації:

1. *Пузняк З.М.* Методика виявлення впливу на достовірність інформації в інформаційному просторі / З.М. Пузняк, Д.А. Шеремет // Сучасний захист інформації. 2017. - №3. – С.50-55;

2. *Пузняк З.М.* Інформаційно-орієнтована модель як реалізація методики виявлення впливу на достовірність інформації в інформаційному просторі / З.М. Пузняк, А.О. Аносов // Сучасний захист інформації. 2017. - №4. – С.68-72;

3. *Пузняк З.М.* Дослідження процесу акустоелектричного перетворення в охоронних датчиках / З.М. Пузняк, М.В. Бржевський // Сучасний захист інформації. 2018. - №2. – С.65-71.

4. *Бржевська З.М.* Вплив на достовірність інформації як загроза для інформаційного простору / З.М. Бржевська, Г.І. Гайдур, А.О. Аносов // Кібербезпека: освіта, наука, техніка. – 2018. - №2(2). – С. 105-112. (Index Copernicus) DOI: 10.28925/2663-4023.2018.2.105112.

5. *Бржевська З.М.* Побудова системи маршрутизації даних в безпроводових сенсорних мережах на основі концепції лавинного розповсюдження (flooding) / Н.М. Довженко, Р.В. Киричок, З.М. Бржевська // Сучасний захист інформації. №4 (36), 2018., С. 17-21 DOI: 10.31673/2409-7292.2018.041216

6. *Бржевська З.М.* Інформаційні війни: проблеми, загрози та протидія / З.М. Бржевська, Н.М. Довженко, Р.В. Киричок, Г.І. Гайдур, А.О. Аносов // Кібербезпека: освіта, наука, техніка. – 2019. - №3(3). – С. 88-96. (Index Copernicus) DOI: 10.28925/2663-4023.2019.3.8896.

7. *Бржевська З.* Дослідження проблематики функціонування алгоритму передачі інформації при наявності прихованих вузлів в

безпроводових сенсорних мережах / А. Бондарчук, З. Бржевська, Н. Довженко, А. Макаренко, В. Собчук // Кібербезпека: освіта, наука, техніка. – Том 4 № 4., 2019. – С. 54-61 (Index Copernicus) DOI 10.28925/2663-4023.2019.4.5461

8. *Бржевська З.* Критерії моніторингу достовірності інформації в інформаційному просторі / З. Бржевська, Н. Довженко, Г. Гайдур, А. Аносов // Кібербезпека: освіта, наука, техніка. – Том 1 № 5., 2019. – С. 52-60. (Index Copernicus) DOI 10.28925/2663-4023.2019.5.5260

9. *Brzhevska Z.* Analysis and design of a hybrid load management method for the IoT networks / Vitalii Savchenko, Volodymir Druzhynin, Mykola Tverdohlib, Yevhen Ivanichenko, Nadiia Dovzhenko, Zoreslava Brzhevska, Valentina Chorna. // International Journal of Advanced Trends in Computer Science and Engineering, 9(1), January – February 2020. – (Scopus Indexed) - ISSN. 2278-3091, P 552 – 557

10. *Бржевська З. М.* Метод контролю послідовності реалізації атакуючих дій під час активного аналізу захищеності корпоративних мереж / Р.В. Киричок, Г.В. Шуклін, З.М. Бржевська // Сучасний захист інформації. №2 (42), 2020., С. 52-58.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

11. *Бржевська З.М.* Вплив на достовірність як загроза для інформації. – Ч Всеукраїнська науково-практична конференція «Актуальні проблеми управління інформаційною безпекою держави». – Збірник тез наукових доповідей Національної академії служби безпеки України. м. Київ, 4 квітня 2019р. – С. 282 - 284

12. *Бржевська З.М.* Аналіз класифікацій загроз інформаційній безпеці держави. – Всеукраїнська наукова конференція: «Актуальні проблеми кібербезпеки». – Збірник наукових тез наукових доповідей Державного університету телекомунікацій. м. Київ, 24 жовтня 2019р. – С. 27-28

13. *Бржевська З.М.* Проблематика розвитку інформаційної безпеки в умовах інформаційного протиборства. – XII Всеукраїнська науково-практична конференція: «Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення. Застосування підрозділів, комплексів, засобів зв'язку, автоматизації та кібербезпеки в операції Об'єднаних сил». – Збірник наукових тез та доповідей Військового інституту телекомунікацій та інформатизації. м. Київ, 3 грудня 2020 р. - С. 104-105

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АСУП – Автоматизована система управління підприємствами

БГВУ – Блок генерування впливу управління

БД – База даних

БУІД – Блок управління ідентифікатором достовірності

БУОТС – Блок управління організаційно-технічної системи

ДЗД – Джерело загроз достовірності

ДІ – Джерело інформації

ЕГ – Експертна група

ЗагДІ – Загрози достовірності інформації

ЗДІ – Забезпечення достовірності інформації

ЗМІ – Засоби масової інформації

ІД – Ідентифікатор достовірності

ІП – Інформаційний простір

ІПр – Інформаційний процес

ІР – Інформаційні ресурси

ІС – Інформаційна система

КІВ – Канали інформаційного впливу

КС – Комп’ютерні системи

НСД – Несанкціонований доступ

ОІ	–	Обробка інформації
ОТС	–	Організаційно-технічна система
ПЗ	–	Програмне забезпечення
ППД	–	Програма підвищення достовірності
ПС	–	Пам'ять стану
РЕБ	–	Радіоелектронна боротьба
СЗДІ	–	Система забезпечення достовірності інформації
СУ	–	Система уразливостей

ВСТУП

Актуальність теми. Зростання інформаційних технологій в усьому світі зумовило, не тільки швидкий розвиток і ефективне застосування інформаційних мереж у підприємницькій діяльності та повсякденному житті, а й появу нових загроз. У сучасному світі, внаслідок постійного зростання значення інформації індустрія її одержання, обробки, реєстрації, передачі та поширення стає однією з провідних галузей діяльності людства, куди з кожним роком вкладають усе більші кошти. Інформація стає найважливішим стратегічним ресурсом, брак якого призводить до істотних втрат у всіх сферах життя.

Виходячи з реалій сьогодення, ефективність функціонування будь-якої організації, підприємства та держави залежить не тільки від надійності функціонування інформаційно - телекомунікаційних систем, а й у значній мірі від захищеності їх інформаційних ресурсів та інформації взагалі [1]. Однією з проблем, яка стримує впровадження ефективних систем захисту інформаційних ресурсів організації чи держави, є проблема створення достовірної класифікації атак та механізмів «фільтрування» інформації, яка проходить від першоджерела до споживача. Зважаючи на це, підвищення ефективності виявлення атак на інформаційні ресурси, залишається актуальним завданням. Систематизація знань про атаки допомагає розробці заходів і систем захисту від них. Тому фахівці в області інформаційної безпеки не припиняють спроб побудови різних класифікаційних схем, які в тій чи іншій мірі сприяють розумінню процесів, що ведуть до проникнення в системи, і допомагають розробляти заходи захисту і реалізовувати системи захисту.

Також, сьогодні як ніколи, є актуальним поняття «інформаційна війна». Всі ми мимоволі стаємо свідками та учасниками різних інформаційних протиборств - чи то передвиборних перегонів, чи то спроб рейдерських атак,

чи то просто просування деяких товарів і послуг у конкурентному середовищі. У класичному розумінні, інформаційна війна – це одна з форм інформаційного протиборства, комплекс заходів щодо інформаційного впливу на масову свідомість для зміни поведінки людей і нав'язування їм цілей, які не відповідають їхнім інтересам, а також, природно, захист від подібних впливів.

Процес передачі інформації від офіційного джерела чи з "місця події" до кінцевого споживача є достатньо складним і тривалим. Під час свого просування інформація циркулює в інформаційному просторі і перебуває під впливом різних груп впливу, які переслідують власні інтереси. Таким чином дуже часто кінцевий користувач отримує упереджену, необ'єктивну інформацію, метою якої є вчинення певного впливу на його поведінку.

Ситуація ускладнюється у випадку обмеженості джерел інформації, їх суб'єктивності та упередженості, які складають сутність інформаційного протиборства, коли протидіючі сторони намагаються будь-що чинити інформаційний тиск як на джерела інформації так і на увесь процес її розповсюдження. Для забезпечення нормального функціонування, прийняття адекватних рішень завданням кінцевого користувача є одержання об'єктивної своєчасної інформації, для чого на передній план виступають питання оцінювання її достовірності.

Питанням інформаційної взаємодії та оцінювання достовірності інформації присвячено значну кількість робіт вітчизняних та іноземних науковців. Так, у роботах Д.А. Губанова, Д.А. Новікова, А.Г. Чхартишвілі розглядається широке коло питань взаємодії користувачів у соціальних мережах. Роботи Г.Г. Почепцова, О.К. Юдіна, Р.В. Грищука, К.В Молодецької, В.П. Городнова, А.П. Верьовченка, В.В. Горчакова присвячені теоретичним та практичним аспектам інформаційного протиборства. Публікації М.Ю. Монахова, Д.А. Полянського, І.І. Семенова, К.Г. Абрамова, І.Р. Конєєва, А.В. Беляєва, Г.І. Гайдур, Н.М. Довженко та ін. присвячені оцінюванню достовірності інформації та її джерел.

Разом з тим, незважаючи на значну кількість публікацій щодо вирішення різноманітних аспектів оцінювання достовірності інформації на сьогоднішній день залишається невирішеною проблема комплексного оцінювання достовірності з урахуванням можливого інформаційного впливу на ресурси та канали передачі інформації.

Основне протиріччя, яке лежить в основі наукового дослідження полягає, з одного боку в тому, що інформація, яка добувається, передається та зберігається, не завжди може бути представлена у вигляді даних чи відомостей на машинних носіях у стандартизованому чи формалізованому вигляді, а, відтак потребує особливих підходів щодо її захисту від спотворення. З іншого боку, вплив інформаційного протиборства, який також є інформаційним, також не може бути представленим методами формальних теорій та числень, що унеможливлює його оцінювання під час оцінки достовірності інформації. Отже, вирішенню підлягає актуальне наукове завдання щодо *розроблення методики оцінювання достовірності інформації в умовах інформаційного протиборства* для захисту інформаційних ресурсів організації та забезпечення інформаційної безпеки користувачів.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконана відповідно до положень Законів України “Про інформацію”, “Про концепцію національної програми інформатизації”, “Про телебачення і радіомовлення”, “Про телекомунікації”; Доктрини інформаційної безпеки України, затвердженої Указом Президента України від 25.02.2017 р. № 47/2017; Стратегії національної безпеки України, затвердженої Указом Президента України від 14.09.2020 № 392/2020, та плану наукової та науково-технічної діяльності Державного університету телекомунікацій у рамках науково-дослідних робіт: “Розробка методів та засобів підвищення живучості інформаційно-комунікаційних систем в умовах впливу кібернетичних атак”, шифр «Живучість К14» (№ ДР 0114U000391), де автором проведено аналіз факторів впливу інформаційного

протиборства на інформаційні ресурси організації та інформаційно-телекомунікаційні системи; “Конкурентна розвідка як складова забезпечення інформаційної безпеки підприємства”, шифр “CompInt”, де автором запропоновано модель процесу управління достовірністю інформації та методику оцінки достовірності інформації в умовах інформаційного протиборства.

Мета і завдання дослідження.

Мета роботи полягає у підвищенні достовірності інформації, яка передається від першоджерела до користувача в умовах інформаційного протиборства.

Для досягнення поставленої мети в дисертації необхідно вирішити такі завдання:

здійснити порівняльний аналіз існуючих методичних підходів щодо оцінювання достовірності інформації в умовах інформаційного протиборства;

розробити математичну модель впливу на інформацію;

розробити модель процесу управління достовірністю інформації в умовах інформаційного протиборства;

розробити методику оцінки достовірності інформації в умовах інформаційного протиборства;

дослідити ефективність методики оцінки достовірності інформації та сформувати практичні рекомендації щодо її застосування.

Об’єкт дослідження – процес передачі інформації від першоджерела до користувача в умовах інформаційного протиборства.

Предмет дослідження – моделі та методи оцінки достовірності інформації в умовах інформаційного протиборства.

Методи дослідження. Дослідження базується на сучасних методах системного аналізу, моделювання та диференційних числень – для удосконалення моделі інформаційного впливу; теорії управління та автоматних граматик – для розробки моделі процесу управління достовірністю

інформації в умовах інформаційного протиборства; теорії нечітких множин та методах експертного оцінювання – для удосконалення методики оцінки достовірності інформації; теорії ризиків – для розробки методики оцінки ризиків порушення достовірності інформації.

Наукова новизна одержаних результатів полягає в тому, що у дисертаційній роботі:

удосконалено математичну модель інформаційного впливу, яка базується на системі диференційних рівнянь, що описують зміну кількості прихильників інформаційних повідомлень у залежності від індивідуальних особливостей соціальних груп та, на відміну від існуючих, додатково враховує можливість забування та особливості засвоєння інформації окремими індивідами групи. Такий підхід дозволяє моделювати вплив на інформацію у процесі її проходження через різні засоби передачі та відтворювати процеси інформаційного протиборства при проходженні повідомлень від першоджерела до кінцевого користувача;

вперше розроблено модель процесу управління достовірністю інформації в умовах інформаційного протиборства, яка базується на моделі скінченного автомата із заданим кінцевим станом достовірності інформаційних повідомлень при відомому початковому стані інформаційних ресурсів і наборові допустимих дій. Такий підхід дає можливість реалізувати багатокрокову перевірку повідомлень з поступовим підвишенням показників достовірності у залежності від характеру повідомлень та ступеня впливу на їх зміст;

удосконалено методику оцінки достовірності інформації в умовах інформаційного протиборства, яка базується на методі експертного оцінювання та, на відміну від існуючих, додатково враховує частоту виникнення факторів інформаційного протиборства та ймовірність спроб порушення достовірності інформації. Така методика дозволяє визначати кількісні та якісні показники достовірності інформації в

інформаційному потоці в умовах впливів, які можуть описуватися як чіткими так і нечіткими змінними;

вперше розроблено методику оцінки ризиків порушення достовірності інформації, яка передбачає встановлення залежності можливого збитку організації, через порушення достовірності вхідної інформації від ступеня впливу конкретного фактора інформаційного протиборства на окремий інформаційний ресурс. Такий підхід дозволяє визначати найбільш доцільні заходи щодо забезпечення достовірності інформації, яка надається такими ресурсами кінцевим споживачам.

Практичне значення одержаних результатів. Нові наукові результати, одержані у роботі, у сукупності складають підґрунтя для створення системи захисту інформації на підприємстві чи організації в умовах інформаційного протиборства.

У роботі наведено комплекс алгоритмів перевірки достовірності інформації, які дозволяють сформувати систему управління інформаційним захистом підприємства на основі реалізації процедур управління достовірністю інформації.

У роботі запропоновано рекомендації щодо удосконалення політик безпеки для організацій різних форм власності, які функціонують в умовах інформаційного протиборства з боку конкурентів та недоброзичливців.

Результати досліджень прийняті до впровадження в ТОВ «IT Спеціаліст» (акт від 09.12.2020 р.), в ТОВ «Євротелеком» (акт від 07.12.2020 р.).

Особистий внесок здобувача. Всі положення, які виносяться на захист, належать особисто автору. У роботах, які опубліковано у співавторстві, особисто здобувачу належать: у [2] розроблено критерії оцінювання достовірності інформації в інформаційному просторі підприємства на основі інформаційно-орієнтованої моделі; у [3] визначено критерії оцінки достовірності інформації в інформаційному просторі та запропонована

методика виявлення впливу на достовірність інформації.; у [4] досліджено канали витоку акустичної інформації та можливості побудови ефективної системи інформаційної протидії такому витоку; у [5] досліджено канали впливу на достовірність інформації та запропоновано методику оцінки достовірності інформації в умовах інформаційного протиборства; у [6] проаналізовано різні способи впливу на інформацію у процесі її поширення у мережі; у [7] описано основні загрози для інформаційного простору держави та визначено механізми протидії впливу на інформаційний контент; у [8] алгоритми безпечної передачі інформації з урахуванням можливості впливу на неї; у [9] пропонуються критерії оцінювання достовірності інформації у інформаційному просторі держави; у [10] запропоновано алгоритм безпечного розповсюдження інформації у мережі в умовах інформаційної протидії.

Апробація результатів дисертації. Основні результати роботи доповідались та отримали позитивну оцінку на:

Всеукраїнській науково-практичній конференції «Актуальні проблеми управління інформаційною безпекою держави» (м. Київ, Національна академія СБУ, 4 квітня 2019 р.);

Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки» (м. Київ, Державний університет телекомунікацій, 24 жовтня 2019 р.);

Всеукраїнська науково-практична конференція: «Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення. Застосування підрозділів, комплексів, засобів зв’язку, автоматизації та кібербезпеки в операції Об’єднаних сил». (м. Київ, Військовий інститут телекомунікацій та інформатизації, 3 грудня 2020 р.).

Публікації. За результатами дисертаційних досліджень опубліковано 12 наукових праць. Основні наукові положення викладено у 9 наукових статтях [2 – 10], серед яких [2 – 9] опубліковані у спеціалізованих фахових виданнях України, [10] опубліковано у закордонному науковому виданні, що входить до

бази SCOPUS. За матеріалами виступів на науково-технічних конференціях опубліковано 3 тез доповідей [11 – 12].

Обсяг і структура дисертації. Дисертація складається зі вступу, 4 розділів, 2 додатків та списку використаних джерел із 124 найменувань на 15 сторінках. Повний обсяг дисертації складає 205 сторінок, з них 157 сторінок основного тексту.

РОЗДІЛ 1.
АНАЛІЗ МЕТОДИЧНИХ ПІДХОДІВ ЩОДО ОЦІНЮВАННЯ ДОСТОВІРНОСТІ ІНФОРМАЦІЇ В УМОВАХ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА

1.1. Аналіз процесу передачі інформації від першоджерела до користувача в умовах інформаційного впливу

Структура інформаційного простору, як середовища інформаційного протиборства. Поняття “інформаційний простір” було сформовано у геополітичному вимірі, що містить властивості й дає можливість розглядати його як самостійні простори із власними ресурсами, структурою, межами та особливостями діяльності, взаємодії суб’єктів, які включають інформаційне забезпечення. Інформаційний простір не є статичним, тому він може швидко адаптовуватись до викликів розвитку сучасного суспільства, стаючи на охороні інтересів держави або, навпаки, впливаючи на неї. Інформаційний простір – це середовище, в якому змінюється зміст таких процесів, як конкуренція (через зміну змісту й характеру конкурентної боротьби між суб’єктами, що діють у ньому) та взаємодія в процесі спільної діяльності.

В інформаційному просторі відслідковуються суттєві зміни характеру геополітичної конкуренції, через боротьбу за досягнення інформаційної переваги, за володіння краще розвиненим інформаційним ресурсом, який може відкрити більші перспективи контролю над інформаційним ресурсом супротивника [13].

На сьогодні, існує чимало наукових підходів до пояснення інформаційного простору. В інформаціологічному аспекті, тлумачення цього

терміна грунтується на визначенні інформаційної сфери. Термін “інформаційний простір” застосовують для вираження системи зовнішніх та внутрішньоорганізаційних потоків інформації, які, у свою чергу, можуть мати різні ознаки з погляду змісту методів, передачі та інтенсивності обміну інформацією. Інформаційний простір також використовують для позначення певної сфери діяльності суспільства, охопленої певною системою потоків інформації [14]. “Сукупність інформації, інформаційної інфраструктури, суб’єктів, що здійснюють збір, формування, поширення і використання інформації, а також системи регулювання певних суспільних відносин, визначається як інформаційна сфера” [15]. Розповсюдженим є підхід до розуміння інформаційної сфери, як сукупності відносин, що виникають при утворенні й використанні інформаційних ресурсів на основі створення, збору, обробки, накопичення, зберігання, пошуку, розповсюдження та надання споживачеві інформації, організація й використання інформаційних технологій та засобів їх забезпечення. Інформаційний простір є динамічним середовищем, де фізичні об’єкти, зазвичай, мають точно визначені фізичні межі, що можуть здобувати інформаційні переваги часу, а простір є структурованим. “Інформаційні поля та інформаційні потоки є основними структурними компонентами інформаційного простору. Рух інформації в інформаційному полі виконується за допомогою фізичного зв’язку між одержувачем і джерелом інформації, що матеріалізується в інформаційному потоці.

Комплекс інформації, що переміщується в інформаційному просторі через канали комунікації, науковці розглядають як інформаційний потік. Інформаційні потоки можуть поширюватися як усередині окремих інфосфер, так і між ними, залежно від наявноств каналів комунікації [15].

Інформаційна інфраструктура суспільства – це середовище, яке забезпечує можливість збору, передачі, зберігання, обробки й розповсюдження інформації. Як складова, вона належить до технологічних й

організаційних компонентів інформаційного простору. “Інформаційна інфраструктура суспільства виникає комплексом: інформаційних і телекомунікаційних систем та мереж зв’язку індустрії засобів інформатизації, телекомунікації і зв’язку; систем формування і забезпечення збереження інформаційних ресурсів; системи забезпечення доступу до інформаційно-телекомунікаційних систем, мереж зв’язку та інформаційних ресурсів; індустрії інформації та ринку інформаційних послуг; системи підготовки кадрів, проведення наукових досліджень; алгоритмів і програмних засобів, що забезпечують функціонування програмно-апаратних платформ тощо” [15].

Інформаційний простір суспільства вирізняється суб’єктами й співтовариствами. Через відсутність меж і своїй віртуальності інформаційний простір є інтеграційним механізмом організаційних структур. Основними функціями, які нині виконує інформаційний простір, є такі: інтегруюча – об’єднання в просторово-комунікативне й соціокультурне середовище різних видів діяльності (економічної, соціальної, політичної та культурної); комунікативна – створення особливого середовища транскордонної, інтерактивної й мобільної комунікації різних суб’єктів, у межах якої вони здійснюють обмін інформації; актуалізуюча визначає об’єктивізацію інтересів різних суб’єктів діяльності в інформаційному просторі через реалізації ними інформаційної політики ; геополітична – формування особистих ресурсів і зміна значущості традиційних ресурсів, створюючи нове середовище геополітичних відносин і конкуренції [15]. Інформаційна сфера є двигуном розвитку постіндустріального суспільства та активно впливає на стан політичної економічної,оборонної та інших складових національної безпеки.

Оскільки інформаційний простір держави на сьогоднішній день став середовищем інформаційної протидії, то, відповідно, усі інформаційні ресурси також можуть бути класифіковані за їх належністю до певних сторін такої протидії. Найбільш яскраво це може бути проіллюстровано на прикладі

медійного простору, який є частиною інформаційного простору держави (рис. 1.1).

Рис. 1.1. Структура медійного простору держави, як середовища інформаційної протидії

Функції інформаційного простору. На сьогоднішній день *Інформаційний простір* (ІП) все частіше розглядається як сфера ведення інформаційного протиборства [16, 17].

Дії в інформаційному просторі розгортаються в [16, 17]:

– технічній сфері;

– психологічній сфері.

Технічна сфера – це область інформаційного простору, в якій створюється, оброблюється та зберігається інформація. Крім того, це область, в якій функціонують системи управління, розвідки та звязку. В подальшому, у списку головних документів, розвиток і уточнення поняття технічної сфери

інформаційного простору призвело до створення понятійного апарату кіберпростір.

Психологічна сфера – область інформаційного простору, яка поєднує мислення конкурентів та суспільства.

Це область, в якій формуються плани конкурентів, доктрини, тактика і методи протиборства, поняття згуртованості, рівень підготовки, мораль, досвід, розуміння ситуації і суспільна думка [16, 17].

Чимало експертів ЗС США вважають доцільним виключення участі фізичних засобів поразки в інформаційних діях (таких як руйнування інфраструктури, невдачі пунктів управління і т.д.), оскільки ці діяння відбуваються в фізичному просторі, яке є звичною областю війни і об'єднує традиційні сфери протиборства – землю, море, повітря і космічний простір. Тобто той простір, в якому функціонують системи військової техніки, озброєння і системи комунікацій [16].

Одним з основних понять, яким оперують спеціалісти в області інформаційного протиборства США, є «інформаційна обстановка», яка по змістовому контексту співзвучна «інформаційному простору».

Інформаційна обстановка – сукупність індивідів, організацій і систем, які збирають, обробляють, доводять інформацію чи діють на її основі [18].

Елементи інформаційної обстановки – керівники, особи, які приймають рішення, індивіди, організації і системи [18].

Ресурси інформаційної обстановки – матеріальні засоби і системи, що використовуються для збору, аналізу, застосування чи спростування інформації [18].

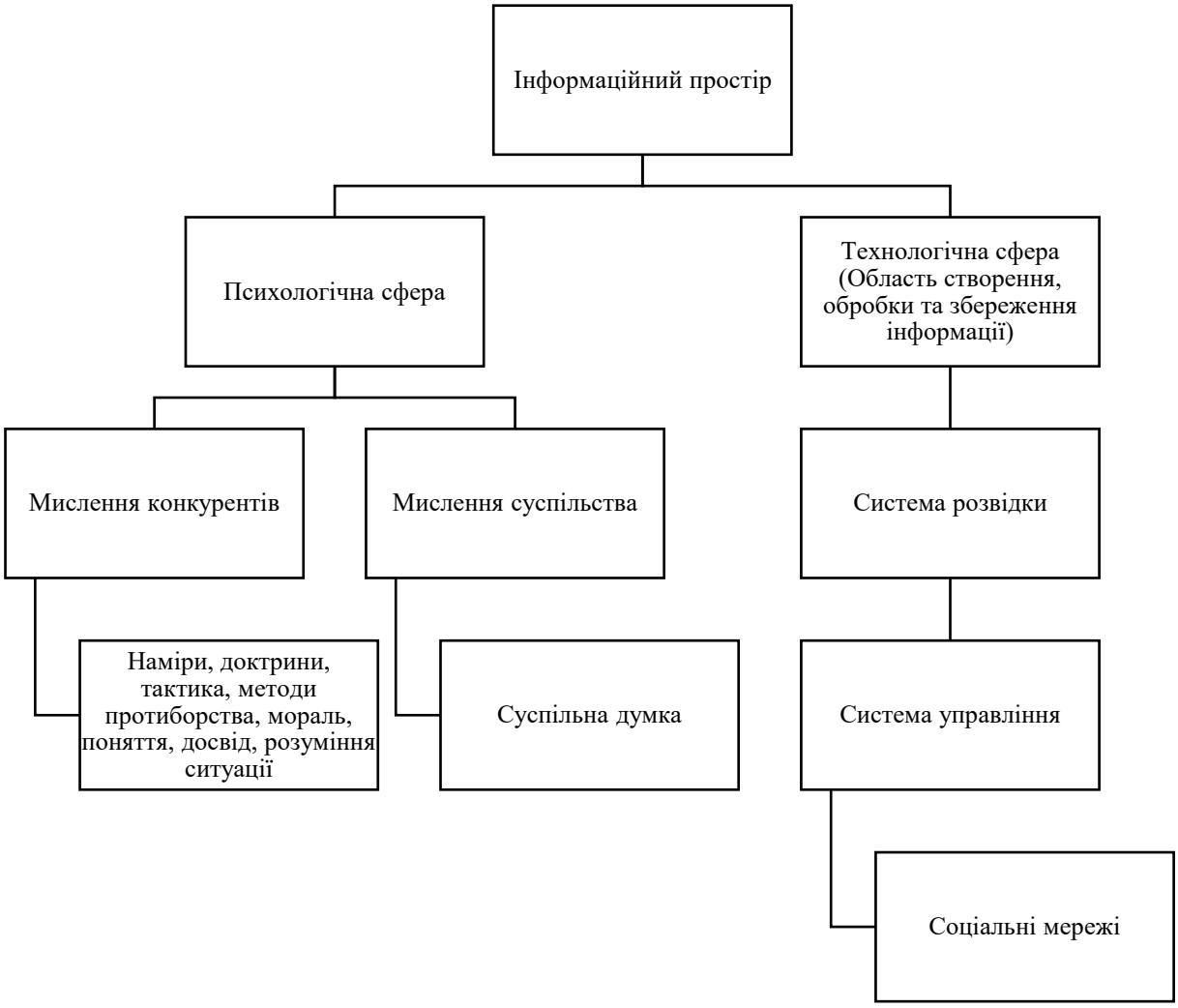

Рис. 1.1. Декомпозиція інформаційного простору [16, 17]

Включаючи поняття ресурсу і елементів, можна надати наступне визначення інформаційної обстановки: це сфера, в якій функціонують індивіди і автоматизовані системи – ведуть спостереження, орієнтуються, приймають рішення і діють на основі інформації. З цієї точки зору, інформаційна обстановка є «основною обстановкою прийняття рішень» в інформативному просторі.

З огляду спеціалістів США, інформаційна обстановка складається з трьох вимірів: фізичного, інформаційного та пізнавального (рис. 1.2) [18]

Фізичний вимір – звична область війни. Ця область об’єднує традиційні сфери протиборства – землю, море, повітря та космічний простір. Ця область, в якій функціонують фізичні платформи озброєння і технічні системи управління і зв’язку. Тому елементи цієї області простіше всього ідентифікувати. Бойова могутність в цій області традиційно вимірюється ефектами фізичної поразки [16, 18].

Інформаційний вимір – область, в якій створюється, оброблюється та зберігається інформація. До того ж, це область, в якій існує логіка функціонування систем управління, зв’язку і розвідки. В суперництві за інформаційну перевагу, ця область є найчутливішою до інформаційних впливів, адже саме цей вимір повязує реальний фізичний світ з логікою функціонування технічних систем збору, передачі і обробки інформації, а через них – з свідомістю людини, яка функціонує в пізнавальному вимірі.

Пізнавальний вимір – область мислення учасника бою та мирного населення. Це область, в якій формується мета командирів, доктрини, тактика, методи протиборства. Нематеріальні активи лідерства,згуртованості підрозділів, рівень підготовки, досвіду, моралі , розуміння ситуації і суспільної думки – це все елементи цієї області. Пізнавальний вимір існує в свідомості індивіда, який приймає рішення. Це та область, де людина обробляє прийняту інформацію у відповідності з властивим йому комплексом норм, моралі, переконань, культури і цінностей. Останні діють в якості основи у сприйнятті індивідом, у фільтруванні ним інформації та визначенні свідомістю значущості та взаємозв'язку. Інформація оцінюється і аналізується, щоб сформувати висновки, які передаються через інформаційний вимір в область фізичного світу [18].

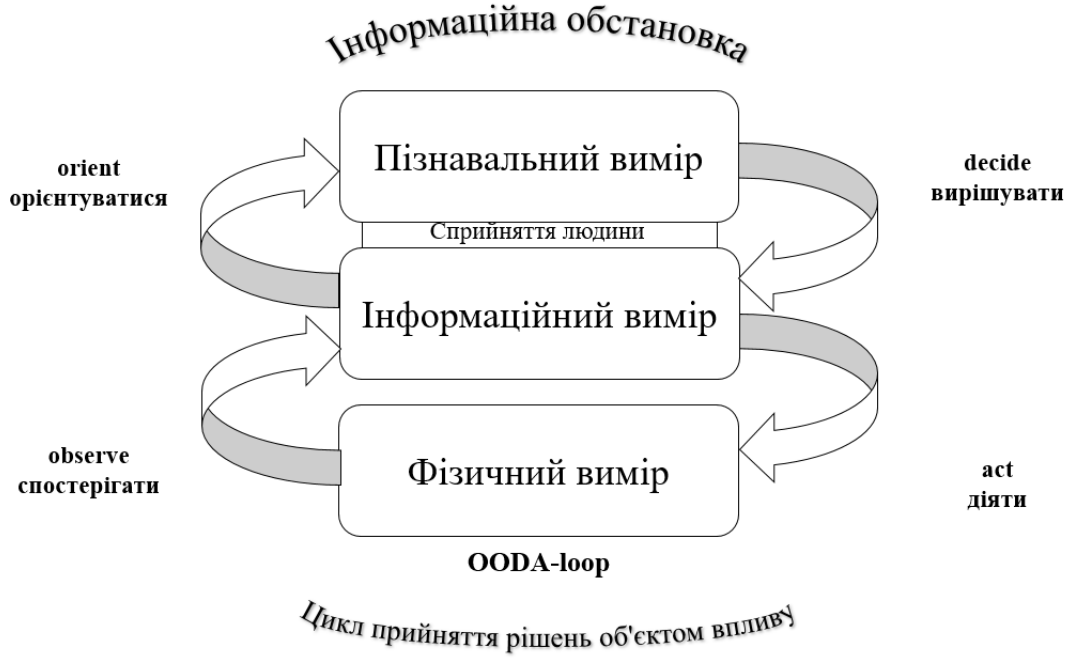

Рис. 1.2. Сфери інформаційної обстановки [18]

Кожна зі складових інформаційної обстановки може піддаватись певному впливу і бути об'єктом, який за певних обставин може вплинути на результат операції (війни) з урахуванням їх концептуального взаємозв'язку в циклі вирішення.

Інформаційний процес комунікації. Трансмітер (шифрувальник), що кодує. Якщо стисло, процес передачі інформації, який зазнає впливу, може бути описано Комунікаційною моделлю Шеннона-Вівера, яка була описана у 1948 році в статті «Математична теорія комунікації». Найголовнішою метою застосування даної моделі було поліпшення технологічної комунікації, переважно телефонної, але згодом Вівер застосував її до всіх видів комунікації. Дана модель зосереджує увагу на акті комунікації між комунікатором та реципієнтом та складається з п'яти головних елементів:

1. Інформаційний ресурс (відправник), що продукує повідомлення;

2. Трансмітер (шифрувальник), що кодує повідомлення спеціальними сигналами, які ущільнюються для передачі через кабелі чи супутники;

3. Канал, до якого адаптується закодований сигнал для передачі інформації;

4. Прийом сигналу та перетворення його на повідомлення. Зворотній процес кодування, що забезпечує ефективний зв'язок між комунікатором та реципієнтом;

5. Отримувач (реципієнт). Кінцеве місце призначення повідомлення. На основі отриманої інформації, реципієнт дає зворотній зв'язок відправнику.

Головною особливістю моделі Шеннона-Вівера є виділення зворотного зв'язку (реакції) реципієнта медіа-повідомлення, який може слугувати індикатором правильного отримання повідомлення. А також доданий компонент комунікаційного процесу – шум. Шум вважається дисфункціональним фактором, що може впливати на повідомлення, коли воно пересувається медіа-каналом, в результаті чого реципієнтом може бути отримане помилкове повідомлення.

У якості такого шуму, у нашому випадку може розглядатися інформаційний вплив на повідомлення, який буде призводити до їх спотворення. Це, у свою чергу, і викликає необхідність оцінювання достовірності інформації, яка приймається користувачем.

Вплив на інформацію може відбуватися на будь-якому з етапів її існування та просування від джерела до користувача.

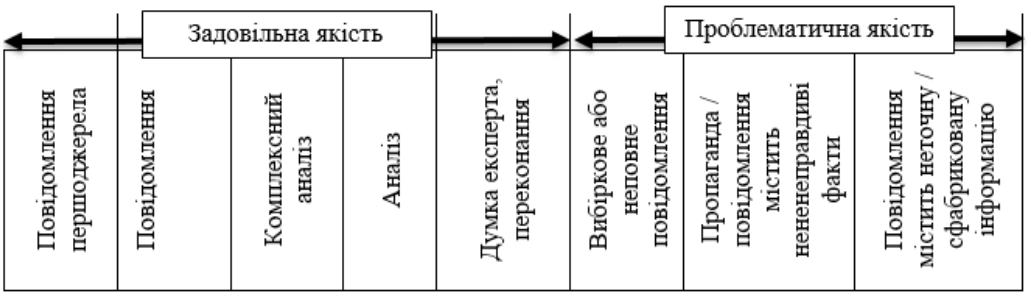

Рис. 1.3. Етапи впливу на інформацію

Отже, інформаційний простір суспільства є результатом його еволюції і утворюється як сукупність інформації, інформаційної інфраструктури та суб'єктів, що здійснюють збір, формування, поширення і використання інформації. На сьогодні, він дедалі частіше розглядається як сфера ведення інформаційної війни у технічному та психологічному доменах. Інформаційний простір є середовищем для здійснення процесу комунікації, який включає інформаційний ресурс, трансміттер, канал комунікації, процедури прийому сигналу та отримувача (реципієнта). На будь-який з цих елементів може чинитися вплив з боку зацікавлених осіб в рамках інформаційного протиборства.

1.2. Аналіз факторів впливу на процеси передачі інформації в умовах інформаційного протиборства

Особливості середовища передачі інформації. Розглянемо особливості (властивості) інформаційного простору, у якому існує необхідність забезпечення достовірності інформації, що передається:

1. «Людський фактор». Виходячи із концепції побудови інформаційного простору (ІП), його слід розглядати як соціо-технічну систему – сукупність інформаційно-технічної та соціальної інфраструктур. За рахунок цього, розширюється базова концепція побудови ІП: в систему, в якості елементів структури відносяться індивіди, а також їхні інформаційні звязки. Основою продуктивного функціонування ІП є не тільки висока продуктивність, надійність і захищеність її апаратно-програмних засобів і персоналу, але і якість інформації (у першу чергу, достовірність), передана і отримана індивідами. Процеси взаємодії індивідів, зумовлені помилковою інформацією, можуть призводити до дисфункціональної поведінки всього ІП [19].

Управління соціального середовища, професійні навики і кваліфікація індивідів, а також загальне розуміння завдань стають важливими складовими ІП, які здійснюють вплив на інформаційні процеси, що зумовлює підхід до забезпечення достовірності інформації, що обробляється.

2. «Конфліктне середовище». Відносини індивідів можуть мати характер конфлікту [20]. Функціонування в конфліктному середовищі означає, що в ІП присутні два динамічні процеси протиборства:

- Процес цілеспрямованого зниження достовірності інформації для переведення ІП в функціонально непостійний стан. Основною причиною його виникнення є інтереси зловмисників, мета яких : спотворити, підмінити, зробити недоступними інформаційні ресурси для «законних» користувачів. Спосіб реалізації – інформаційні атаки. Спроможність їх вдалої реалізації базуються на слабких ланках технічної та соціальної підсистем;

- Процес покращення достовірності інформації, що полягає в виборі «надійних» джерел, для протидій атак зловмисників, відновлення уражених інформаційних ресурсів, забезпечення надійного функціонування технічної та соціальної підсистем.

3. «Багатомасштабність». Інформаційний простір утворюється з багатомасштабних систем [21], які містять багато індивідів і можуть об‘єднуватись в світову систему інформаційної взаємодії. Інформаційні простори можуть бути взаємно проникаючими. Процеси в ІП реалізовані на основі розподілених додатків, можуть проходити з різною швидкістю і мали вплиа один на одного. Також, інформаційні ресурси можуть додаватися і зникати, у процесі функціонування ІП. Забезпечення достовірності інформаційних ресурсів досягається в важко контролюючому середовищі і потребує застосування самопристосовних засобів управління.

4. «Багатозв'язаність». ІП, як правило, багатозв'язкові. Це полягає в відмінності їх елементів , які з'єднані між собою (індивід - інформаційно, апаратно-програмні засоби - фізично) і можуть мати як прямі, так і зворотні

зв'язки. Характер інформаційних зв'язків в ІП [22] сильно залежить від психофізіологічного, інтелектуального та інших станів індивідів. Загальна структурна надійність системи і її компонентів зовсім не означає стійкості ІП, навпаки, в разі поширення неправдивої інформації, може бути змінена мета систем, а нові інформаційні процеси будуть розглядатися як «дизфункціональність», системна нестійкість.

5. «Самоорганізація». ІП можуть бути самоорганізуючі, тобто схильними до самостійної автономної (не керуючими ззовні) появи і поведінки. Це означає, що у ІП з'являється здатність, з одного боку, стати «носій дезінформації», з іншого - виробляти заходи до самозбереження і протидії зовнішнім впливам [23]. Кластери вузлів ІП з зміненим цілеспрямуванням, що частково або повністю втратили санкціоноване управління в результаті атакуючого впливу і захопили ресурси, можуть здійснювати вагомий вплив на забезпечення достовірності інформації в конкретній ІП.

Резюмуючи виділені властивості середовища, відзначимо наступні особливості управління процесом забезпечення достовірності інформації в ІП:

- процес забезпечення достовірності інформації є погано формалізованим об'єктом управління внаслідок того, що перебуває в умовах суттєвої невизначеності, джерелом якої є технічна і соціальна складові ІП. Невизначеність пов'язана з багатомасштабністю і неміцною структурованістю ІП, що з високою складністю відбуваються в системі інформаційних процесів, їх неточністю і недостатньою вивченістю. Також важливо згадати про неодноразову неможливість кількісного виміру значеннь вхідних і вихідних параметрів підсистем, їх високим взаємним впливом, що призводить до синергетичного ефекту [24] і виникнення властивостей емерджентності [25]. Це викликає складнощі (а іноді і неможливості) побудови формальних (аналітичних) моделей окремих процедур управління процесом забезпечення достовірності інформації, що враховує специфіку ІП;

- наявність «людського фактора» призводить до того, що більшість характеристик достовірності інформаційних ресурсів втрачають свою строгу визначеність: зв'язки між соціальною і технічною підсистемами описуються нечітко, залишається відкритим питання про кількість і склад вхідних даних, оскільки невідомо, що може вплинути на поведінку індивіда як елемента системи і т.д. Ефект впливу управляючих впливів на людину є важко передбачуваним. Через те, що мета системи формулюється особою, що приймає рішення, або визначається системою більш високого рівня якісно (тобто нечітко), то це призводить до розмитості, появи «діапазону допустимості» при досягненні мети в управлінні процесом забезпечення достовірності інформації;

- якщо для зняття «невизначеності» при дослідженні технічної підсистеми застосовні класичні методи статистики, то для соціальної підсистеми вони не придатні, оскільки невизначеність в даному випадку носить суб'єктивний характер.

На відміну від об'єктивної ймовірності, яка відображає відносну частоту появи якої-небудь події в загальному обсязі спостережень, під суб'єктивною ймовірністю розуміється міра впевненості людини або групи людей (експертів) в тому, що дана подія в дійсності буде мати місце.

Таким чином, управління процесом забезпечення достовірності інформації в ІП слід розглядати як складний інтелектуальний процес розв'язання проблем, який не може зводитися виключно до раціонального вибору. Для підтримки цього процесу доцільно використовувати когнітивний підхід до моделювання і управління, оскільки він спрямований на розробку формальних моделей і методів, що підтримують інтелектуальний процес вирішення завдань управління, завдяки врахуванню в цих моделях і методах когнітивних можливостей людини [26].

Відповідно до моделі якості інформаційної системи, наведеної в [27] можна виділити основні класи елементів в системі, що впливають на

достовірність інформаційних ресурсів. Об'єднавши ці класи елементів з класом інформаційних джерел і визначивши критерії, за якими можна отримати кількісну або якісну (в поняттях нечіткої логіки) оцінку взаємодії елементів і сили впливу друг на друга, отримаємо наступну когнітивну карту (рис. 1.4).

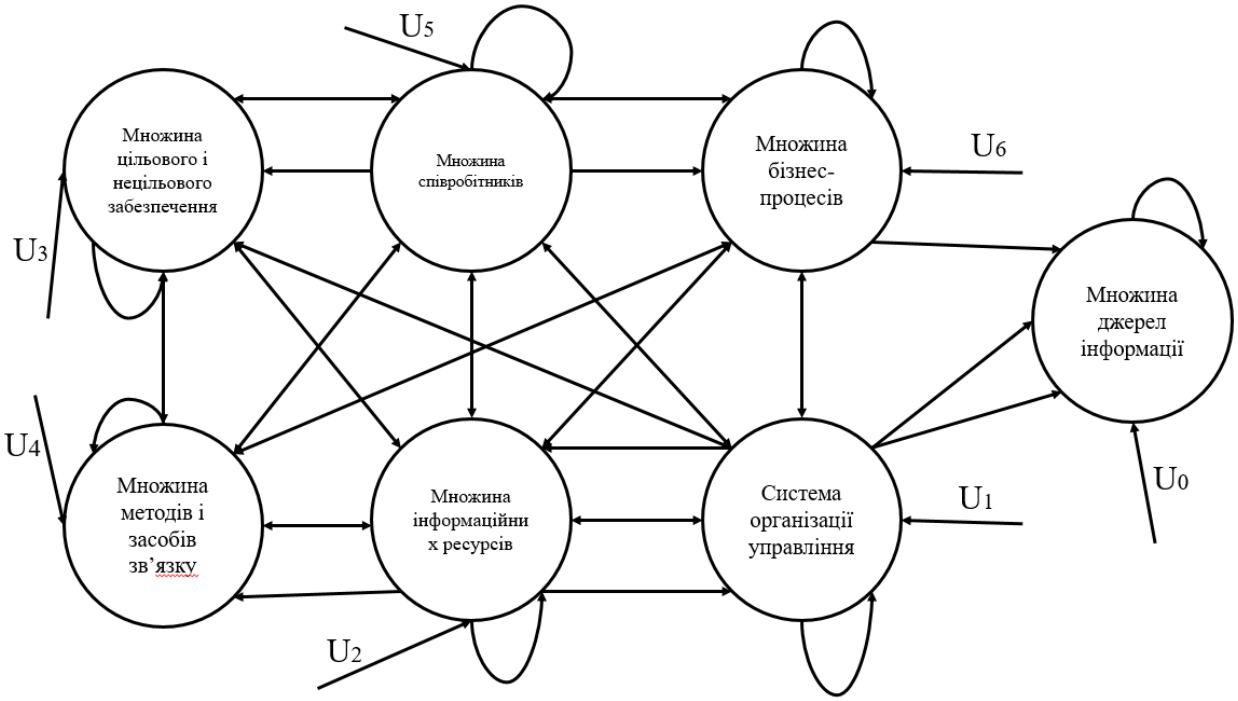

Рис. 1.4. Схема взаємовпливу класів елементів в соціальних комунікаціях

На рис. 1.4. $U_j, j = \overline{0..6}, U_j \in [-1, 1]$ – це впливи на елементи системи, зі сторони зовнішнього середовища або спеціальні заходи, з метою зміни ситуації в роботі системи, $r_i, i = \overline{1..8}, r_i \in [-1, 1]$ - це вагові коефіцієнти, що відображають силу впливу одного параметра на інший, в яких знак мінус вказує на обернено пропорційну силу впливу, *IS*, *IR*, *MS* - критерії, описані на рис. 1.5 і визначаються в межах від 0 до 1.

Початкові оцінки критеріїв можна отримати, маючи:

- дерево з експертними оцінками впевненості в джерелах інформації, які використовуються на підприємстві;

- дерево оцінки впевненості в збереженні / непідверженності загрозам джерел інформації;

- оцінки стандартизації бізнес-процесів;

- імовірнісні оцінки впливу зовнішнього середовища через U_j.

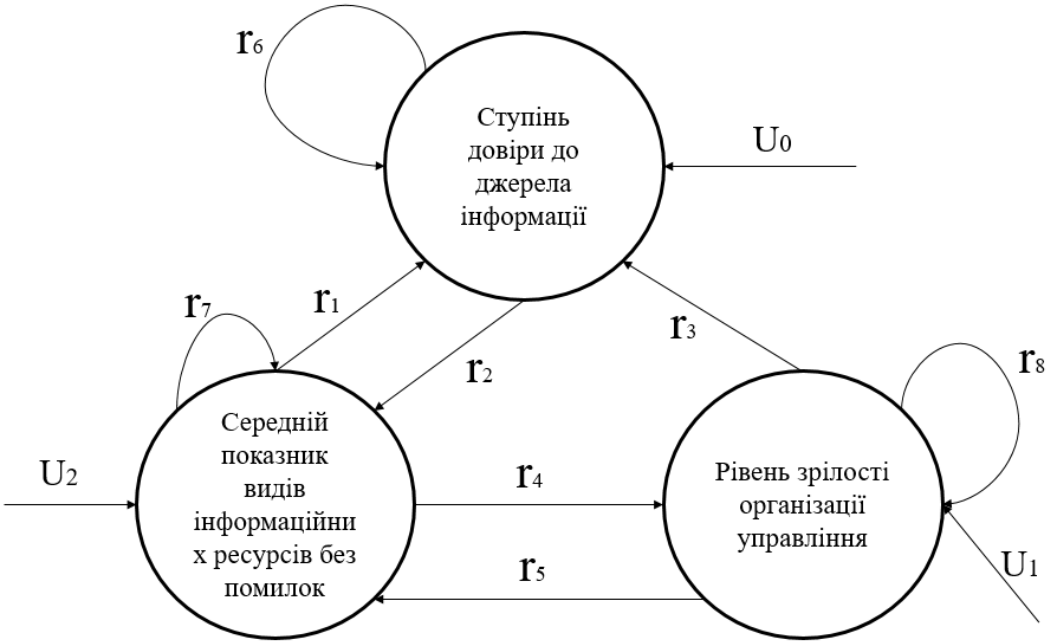

Рис. 1.5. Фрагмент когнітивної карти

Аналіз сценаріїв розвитку ситуації може бути виконаний з застосуванням імпульсного моделювання [26].

Другий підхід базується на системній динаміці, в тому числі, як показано в [15]. Для оцінювання ризиків недостовірності джерела інформації, можливо застосувати модифікацію моделі Вольтера, із врахованням обмеження ресурсів росту і самообмеження максимального значення. Наприклад, розглянемо фрагмент когнітивної карти (рис. 1.5). В результаті експериментів, була визначена одна з форм системи диференціальних рівнянь:

$$\begin{cases} \dfrac{d(IS)}{dt} = r_6 \cdot IS + r_1 \cdot \dfrac{IS}{1+MS} + r_3 \cdot IS \cdot MS + r_9 \cdot IS^2 + U_0; \\ \dfrac{d(IR)}{dt} = r_7 \cdot IR + r_2 \cdot \dfrac{IR}{1+MS} + r_5 \cdot IR \cdot MS + r_{10} \cdot IR^2 + U_2; \\ \dfrac{d(MS)}{dt} = r_8 \cdot MS + r_4 \cdot \dfrac{MS}{1+IR} + r_{11} \cdot MS^2 + U_1. \end{cases}$$

Члени з коефіцієнтами r_3, r_5, r_9, r_{10}, r_{11} відповідають за самообмеження IS, IR, MS. Другі члени рівнянь регулюють швидкість росту значень IS, IR, MS. $r_9 \in [0,1], r_{10} \in [0,1], r_{11} \in [0,1]$ – коефіцієнти в членах рівнянь, що відповідають за спрацювання ферхюльстового фактора.

Інформаційна зброя. Нині, до інформаційної зброї відносять широкий клас прийомів і засобів інформаційного впливу на противника – від дезінформації і пропаганди до засобів радіоелектронної боротьби. При цьому, на сьогоднішній час немає єдиного визначення поняття «інформаційна зброя». В різних джерелах надаються різні визначення цього поняття. Проте в роботі [13] автори надали узагальнене та конкретизоване визначення інформаційної зброї.

Інформаційна зброя – це сукупність способів і засобів [29]:

- подавання елементів інфраструктури державного і військового управління противника;

- радіоелектронний вплив на елементи інформаційних систем;

- несанкціонований доступ до інформаційних ресурсів з подальшою їх деформацією, знищенням чи викраденням;

- інформаційно-психологічні впливи на військовослужбовців та цивільне населення протиборчої сторони.

Сучасна стратегія застосування інформаційної зброї базується на моделі «п’яти кілець» Дж. Вардена. До пяти «центрів тяжіння», в цьому випадку, відносять: керівництво країни і систему державного управління, виробництво, транспортну мережу, населення та збройні сили. Інформаційна зброя може

бути застосована проти всіх елементів цієї моделі. До того ж, максимальна ефективність її використання досягається проти індустріально розвиненого та географічно сконцентрованого противника.

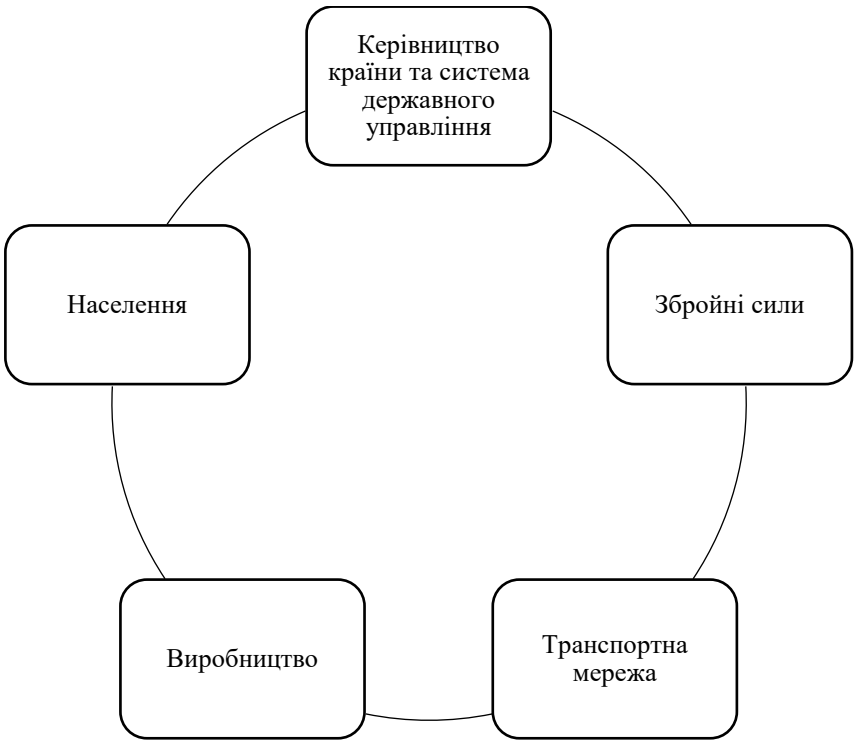

Рис. 1.6. Модель «п’яти кілець» Дж. Вардена

У відповідності зі сферою свого застосування інформаційна зброя класифікується на [29]:

- інформаційно-технічна зброя;
- інформаційно-психологічна зброя.

У відповідності з цільовим призначенням інформаційна зброя класифікується на два типи [29]:

- оборонна інформаційна зброя (вирішує задачі оборони в інформаційній війні і включає системи багаторівневої комп’ютерної безпеки і різні системи активної протидії інформаційно-психологічній зброї противника);

- наступальна інформаційна зброя (вирішує задачі впливу на систему прийняття рішення противником шляхом ураження найбільш критичних з вхідних в неї компонентів).

На рис. 1.7 розглянемо види інформаційної зброї на основі інформаційних технологій.

Засоби впливу на інформаційні ресурси та апаратно-програмні засоби
• засіб подолання систем захисту інформації; • засоби проникнення в інформаційні системи (ІС) противника; • засоби маскування джерел отримання інформації; • засоби виведення з ладу ПЗ інформаційної системи; • засоби прихованого часткової зміни алгоритму функціонування ПЗ; • засоби збору даних, що циркулюють в ІС противника; • засоби доставки і впровадження певних алгоритмів в конкретне місце інформаційної системи; • засоби впливу на системи охорони об'єктів
Засоби впливу на процес передачі інформації
• засоби впливу на протоколи передачі даних систем зв'язку і передачі даних; • засоби впливу на алгоритми адресації і маршрутизації; • кошти перехоплення і порушення проходження інформації в технічних каналах її передачі; • кошти виклику перевантаження системи помилковими запитами на встановлення зв'язку
Засоби психологічного впливу, дезінформації та пропаганди
• вплив за допомогою ЗМІ; засоби пропаганди; засоби створення або модифікації віртуальної реальності; • засоби імітації голосів операторів систем управління і відео зображення конкретних людей з їх голосом (керівників держав, лідерів політичних сил та ін.); • засоби модифікації інформації, що зберігається в базах даних ІС противника; • засоби введення в ІС противника неправдивої інформації і даних (цілевказівки, місць доставки вантажів і ін.); • засоби дезінформації охоронних систем; • засоби модифікації даних навігаційних систем, систем точного часу та ін.
Засоби спеціальних психологічних впливів
• спеціальна відеографічна і телевізійна інформація; • засоби створення віртуальної реальності, яка пригнічує волю людини і викликає страх; • «зомбування» і нейролінгвістичне програмування

Рис. 1.7. Види інформаційної зброї на основі інформаційних технологій

Інформаційно-технічна зброя – сукупність спеціально організованої інформації, інформаційних технологій, способів і засобів, що дозволяють цілеспрямовано змінювати (знищувати, спотворювати), копіювати, блокувати інформацію, обходити системи захисту, обмежувати доступ законних користувачів, дезінформувати, порушувати функціонування систем обробки інформації, здійснювати дезорганізаційну роботу технічних засобів, комп'ютерних систем, а також іншої інфраструктури високотехнологічного забезпечення життя суспільства і функціонування системи управління державою, що використовуєтьсч в ході інформаційної операції для досягнення поставлених цілей.

Інформаційно-психологічна зброя – засоби і способи впливу на потенційного противника, за рахунок маніпуляції інформацією в інтересах формування еліт з заданим світоглядом, прищеплення громадянам певних цінностей і стереотипів, що дозволяють, з однієї сторони, передбачити його поведінку та грати на внутрішніх протиріччях, а з іншої – керувати процесами прийняття рішень на всіх рівнях управління.

До основних засобів інформаційно-психологічної зброї, які набули маштабне розповсюдження, можна віднести (рис. 1.8) [30, 31]:

- друковані матеріали – плакати, листівки, інформаційні бюлетені та інші засоби їх виготовлення (поліграфічна база) і поширення;

- засоби масової інформації – телебачення, радіо, газети, сайти новин та агрегатори новин в мережі Інтернет;

- інтернет-ресурси: спеціально створені сайти; соціальні мережі, чати, блоги, форуми та ін.;

- когнітивна зброя.

Аналіз здійснення на сучасному етапі психологічних операцій, в рамках інформаційного протиборства, дозволяє виділити декілька основних тенденцій розвитку засобів інформаційно-психологічної зброї і способів її

використання, які в найближчому майбутньому визначатимуть її сутність та характер [30].

Далі засоби інформаційно-психологічної зброї і тенденції їх розвитку розглянемо більш детально.

Засоби масової інформації. Засоби масової інформації містять в собі розширений функціональний вплив на психіку індивіда та мас, з ціллю наповнення підсвідомості психологічними установками і формування патернів поведінки в мимовільній психіці. До засобів масової інформації відносяться телебачення, преса, радіо, всі видовищні заходи і література, відеофільми, реклама – все те, завдяки чому можна впливати на масову аудиторію.

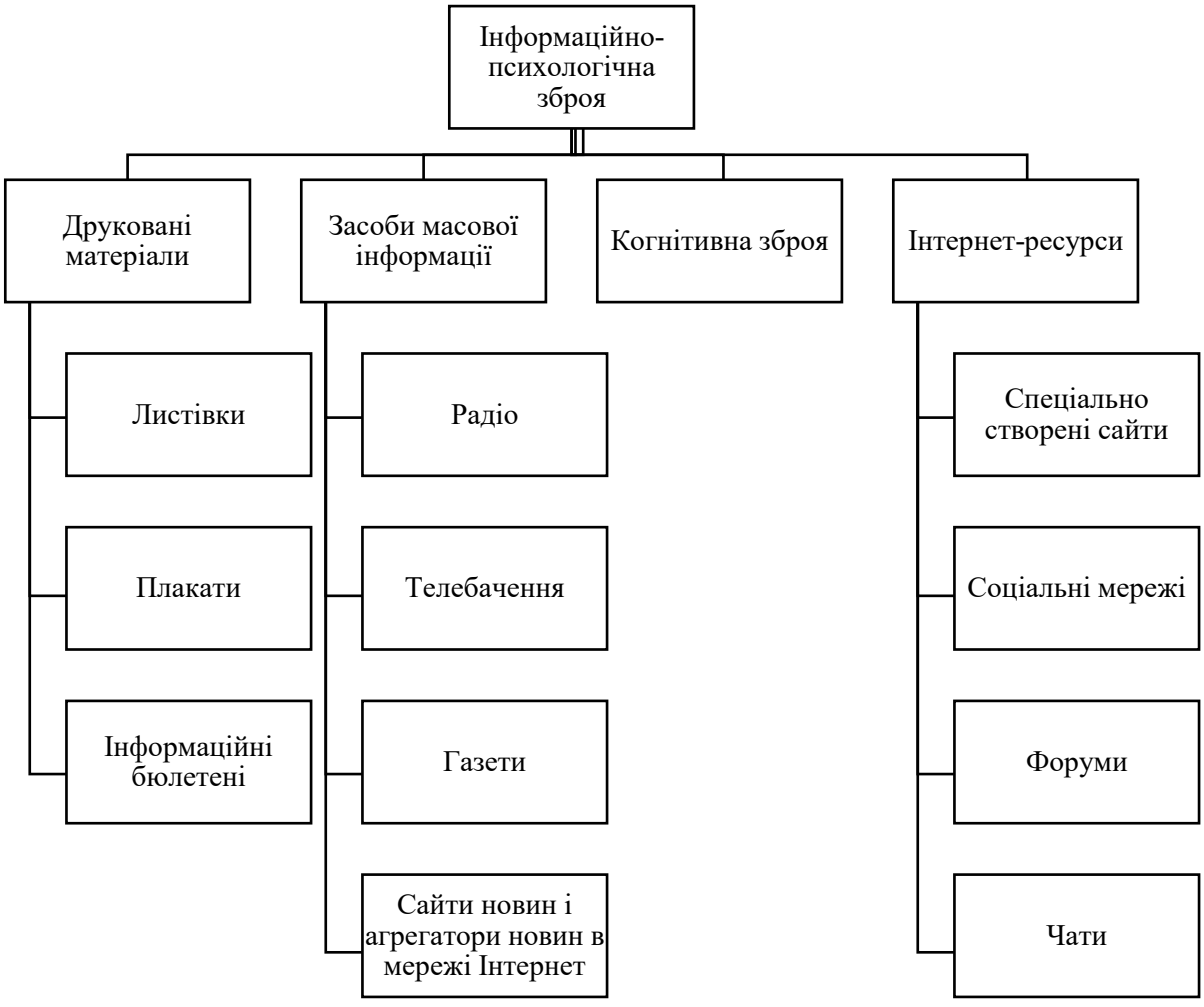

Рис. 1.8. Класифікація засобів інформаційно-психологічної зброї

Основними способами маніпулювання інформацією, що використовується ЗМІ, є:

- відверта брехня з метою дезінформації;

- прикриття критично важливої інформації;

- заглиблення цінної інформації в масив інформаційного сміття;

- спрощення, ствердження і повторення (навіювання);

- підміна термінології: застосування понять і термінів, незрозумілого сенсу, або із якісними змінами, що ускладнює формування реальної картини подій;

- введення заборони на визначені види інформації і розділи новин;

- пізнавання образу: відомі політичні діячі, представники шоу-бізнесу можуть брати участь в замовних акціях, показуючи тим самим певний вплив на світогляд їх шанувальників;

- подача негативної інформації, яка краще сприймається аудиторією в порівнянні з позитивними новинами.

Засоби на основі інтернет-ресурсів та соціальних мереж. В інтересах психологічних операцій, все активніше і масштабніше, застосовуються електронні ЗМІ, а також мережа Інтернет. Діапазон використання мережі Інтернет є доволі широким. Він надає широкі можливості для надання впливу на формування громадської думки, прийняття політичних, економічних та військових рішень, впливу на інформаційні ресурси противника та розповсюдження спеціально підготовленої інформації (дезінформації) [32]. Чималі переваги використання мережі Інтернет перед звичайними засобами спричинені наступними факторами, розглянутими в роботах [16, 32].

1. Оперативність. Розміщення і регулярне оновлення інформації на окремих сторінках, в інтернет-виданнях і різного роду новинних розсилках, форумах і конференціях потребують мінімальних витрат часу для підготовки матеріалів. При цьому користувачі отримують її в режимі реального часу, а цілеспрямований вплив на інформаційні ресурси протилежної сторони може

здійснюватися не тільки в заздалегідь запланований час, але і в міру виникнення необхідності.

2. Економічність. Для вирішення поставлених завдань залучається мінімальна кількість персоналу і матеріальних засобів. До того ж, застосування комп'ютерних технологій для виведення з ладу систем управління противника, при певних умовах, може призвести до більш вагомого ефекту, при значно менших витратах, в порівнянні з використанням традиційних засобів вогневого ураження і РЕБ.

3. Скритність джерела впливу. Оскільки акт агресії в глобальній мережі важко, а часом неможливо відрізнити від звичайних несанкціонованих дій, то підготувати і виконати психологічну операцію з використанням ресурсів мережі Інтернет, може досить широке коло осіб - від спеціальних структур іноземних держав до партизанських формувань.

4. Дистанційний характер впливу на інформаційні системи в різних регіонах світу. Для здійснення інформаційно-психологічного впливу не обов'язково перебувати безпосередньо в місці впливу. Віддалено, коментуючи місцеві новинні канали, маніпулюючи подачею і емоційним сприйняттям інформації, можна забезпечити цільовий інформаційно-психологічний вплив у заданому місці і в заданий час, з будь-якого місця Землі.

5. Масштабність можливих наслідків. Використання глобальної мережі для деструктивних інформаційно-психологічних впливів може призвести до порушення правильної роботи органів державного і військового управління, спровокувати масштабні протести, акції громадянської непокори в окремих районах, країнах або регіонах.

6. Комплексність подачі інформації та її сприйняття. Текстову і графічну інформацію на інтернет-сторінках розміщують в найбільш зручному для сприйняття вигляді, а її обсяг може бути в багато разів більше, ніж у будь-якого друкованого видання, радіопередачі або телевізійної програми. Крім цього, використання сучасних мультимедійних технологій, що дозволяють

демонструвати документальні свідчення та факти, фото- і відеоматеріали при спеціально підібраному супроводі (коментарі, музика), сприяють спеціальному емоційному і психологічному впливу.

7. Доступність інформації. За наявними даними, загальна кількість користувачів Інтернету на кінець 2020 року становить близько 4,3 млрд осіб. Ці люди практично миттєво можуть отримати доступ до інформації, наявної на серверах різних країн, обійшовши стороною прикордонні, цензурні та інші бар'єри. Водночас будь-який користувач може розмістити власну інформацію на серверах, зареєстрованих в інших державах, або організувати розсилання повідомлень по всьому світу. Після кольорових арабських революцій в ЗМІ активно просувалася думка про те, що ці події стали можливими в тому числі виключно завдяки новітнім інтернет-технологій інформаційно-психологічного впливу.

Отже, можна приписувати Інтернету більшу або меншу залежність в сучасних психологічних операціях, але заперечувати її неможливо [32].

Соціальні мережі в мережі Інтернет є сучасним засобом, який використовують в інтересах активації протестуючих настроїв, координації дій протестувальників, надання громадянству інформації про події, що відбуваються.

Когнітивна зброя. Ще однією категорією інформаційно-психологічної зброї є когнітивна зброя, яка дещо відрізняється по своєму впливу від попередньо розглянутих типів.

Когнітивна зброя – це доповнення в інтелектуальне середовище країни-противника неправдивих наукових теорій, парадигм, стратегій, концепцій, що можуть вплинути на його державне управління в сторону зниження оборонно-значимих національних потенціалів [30].

В практичному застосуванні неправдиві наукові теорії, парадигми, концепції, стратегії перетворюються в зброю великої рушійної сили, яка

уражає національну науку і освіту, державне управління, оборону та економіку. [30].

Прикладами когнітивної зброї є: теорія постіндустріалізму; теорія монетаризму; теорія радикального лібералізму в економіці; концепція випередження продуктивності праці по відношенню до оплати праці (в умовах зниженої заробітньої оплати); міграційна тематика; тематика реорганізації контуру освіти та ін. Крім того, поруч з неправдивими політичними та економічними теоріями, спеціалістами по психологічним операціям може здійснюватися внесення неправдивих відомостей про тенденції розвитку сучасної та воєнної науки з метою направити наукові дослідження по неправильному шляху [30].

Таким чином, особливостями інформаційного простору, які впливають на процеси передачі інформації у ньому, є інформаційне протиборство, яке включає: вплив людського фактора, наявність конфліктів, багатовимірність, багатозвязність та самоорганізацію. Одним з визначальних – є вплив на інформацію інформаційної зброї, яка включає широкий клас прийомів і засобів інформаційного впливу – від дезінформації і пропаганди до засобів радіоелектронної боротьби. Інформаційна зброя реалізується через технічні засоби (віруси та інше шкідливе програмне забезпечення, APT-атаки та фізичний вплив на інформаційні системи) та засоби інформаційно-психологічного впливу: друковані матеріали, засоби масової інформації, інтернет-ресурси, когнітивну зброю. Можливість впливу на інформацію реалізується на будь-якому з етапів її існування – від зародження (спостереження, опису, фіксації фактів) до моменту доставки до кінцевого споживача.

1.3. Дослідження науково-методичних підходів оцінки достовірності інформації

Аналіз робіт з проблемами підтримки достовірності інформації в інформаційному просторі організації або держави дозволяє виокремити наступні особливості, принципові для цього дослідження. У літературі представлений широкий спектр методів оцінки і підвищення достовірності інформації. В іноземних публікаціях [29, 33, 34, 35] під достовірністю інформації, як правило, розуміють ознаку інформації, як сприятливість її для використання в завданнях управління прийняттям рішень. Управління якістю даних зумовлює вектор розвитку інформаційного суспільства [36]. Ефективна робота системи планування ресурсів підприємства, багато в чому, залежить від якості даних [37].

Значимість правильної оцінки якості інформації постійно зростає, в силу того, що небезпека наслідків помилкових рішень, на основі недостовірних даних може бути різною: від тимчасових, фінансових і репутаційних втрат до конфліктів і воєн [38]. Проблема якості інформації важлива, в значенні критичної ролі, яку відіграє інформація в економіці, заснованій на знаннях і великих обсягах даних [39].

Інтенсивний розвиток всесвітніх мереж, як середовища для обміну інформацією та відсутність правових стандартів щодо інформації, яка в ньому міститься, призвели до зниження рівня достовірності інформування. Користувачі глобальних мереж беруть участь у взаємодії з чимраз різноманітнішою інформацією, що спричиняє зростання потреби в фільтрації інформації.

Суттєвим аспектом проблеми є нездатність пошукової технології визначити, з великого простору, сумнівний зміст і повернути «якісні» результати запиту користувачу [40, 41].

Врахована якість споживчої інформації є найбільш значущим чинником для прогнозування поведінки споживача [42]. Оцінка ступеня достовірності інформації, з боку користувачів, загалом, заснована на когнітивної оцінці. Фактори, що впливають на судження, визначаються на основі характеристик інформаційних ресурсів, характеристик джерел, знання, ситуації і загального припущення [43].

Встановлені для користувача критерії для визначення якості даних різні і відображають об'єктивні особливості даних і виробничого процесу. Зважаючи на ці показники, користувач може оцінити якість даних для конкретної області застосування [44].

Досягнення необхідного рівня достовірності - складніше і ширше завдання, ніж забезпечення надійності функціонування засобів обробки інформації [5]. Засоби пошуку та виправлення помилок, при обробці інформації в обчислювальних системах, використання надійних і дорогих сховищ даних, не вирішують основну проблему низької достовірності даних [9].

Незважаючи на те, що існує багато досліджень з різних аспектів якості та достовірності інформації, залишається потреба в методології оцінки достовірності інформації, загальної для різного виду ІС, що дозволяє забезпечити основу розвитку інформатизації суспільства [45].

Останнім часом, зросла кількість додатків, які використовують джерела даних, доступних в Інтернеті. Одна з основних проблем, пов'язана з перебуванням найбільш відповідних джерел даних для цього додатка. У загальному випадку, джерело даних вважається релевантним, коли він відповідає запитам, зазначеним в додатку. Однак, може трапитися так, що певне джерело даних відповідає на запит, але відповідь, що виробляється джерелом даних, насправді, не відповідає вимогам користувача [46]. Джерела інформації, використаної в одній інформаційній системі, найчастіше перекривають один одного і формують суперечливу інформацію. Конфлікти

значень в розбіжних джерелах, часто систематичні і викликані деякими властивостями різних джерел [47]. Довіра до інформації проявляється в двох рівнях: інституціональному (домен, визначений URL, тип установи) і індивідуальному (ідентифікація автора, авторська приналежність і ім'я автора) [48].

Дослідження предмету оцінки та підвищення рівня достовірності інформації в інформаційних системах, має грунтуватися на їх аналізі, в якості підсистем, представлення в більш широкі системи управління зі зворотним зв'язком.

Достовірність інформації не є відокремленою характеристикою, а визначає фактори ризиків, які безпосередньо впливають на прийняття рішень [49, 50]. Достовірність інформації іноді розуміють, в дуже обмежених рамках, як точність. Водночас, існує і контекстна якість інформації (відповідність поставленому завданню) [51-53].

Контекстні оцінки настільки ж важливі, як об'єктивні індикатори якості, тому що вони впливають на те, яка інформація застосується для прийняття рішень. Для людини характерний подвійний процес пізнання, який дозволяє одночасно оцінювати як об'єктивні, так і контекстні характеристики інформації [54]. Один і той же ресурс може мати прийнятний рівень якості для деяких контекстів, але він може бути неприйнятним для інших. Однак, існуючі метрики якості даних, в основному, отримують нейтрально, без урахування специфіки контексту. Це свідчить про необхідність перегляду показників якості даних та методів вимірювання для включення оцінки контексту [55]. Якість джерела даних є суттєвим для загального рівня достовірності. Особливо, це актуально для систем, що вимагають спочатку «невизначених» даних [56].

Користувачі, які потребують інформації для досягнення цілей, отримують сукупність інформації, яка містить дефекти. Отримання високого рівня можливе, тільки шляхом виправлення самого потоку, а не усунення

окремих дефектів [57]. Водночас, на дослідження достовірності інформації впливає невизначеність параметрів зовнішніх інформаційних систем та інформаційного обміну [58].

Основним обмеженням наявних підходів до оцінки даних є їх спеціалізація з конкретних питань або умов [59].

Методи оцінки достовірності інформації можна розділити на дві великі групи: евристичні (використовуваними аудиторами) і формальні (оперують моделями інформаційних ресурсів, інформаційних процесів і інформаційних систем [60].

Підходи до оцінки достовірності даних в базах даних (БД) засновані на аналізі відносин і розглядають БД як графа сутність-зв'язок, де прямі і непрямі відносини відповідають шляхах в графі [61]. Тимчасом як звичайні помилки в БД, такі як неіснуючі індекси, можуть бути виявлені і кориговані, за допомогою традиційних інструментів очищення даних, багато помилок, звичайних для виробничого процесу, не можуть бути вирішені. Розв‘язанням проблеми може служити матриця якості в задачах класифікації інтелектуального аналізу даних [62].

Пошук недостовірних даних, навіть при наявності їх високої структуризації і позначених взаємозв'язках (як, наприклад, в реляційному поданні даних) вимагає великий комплекс методів: профілювання даних [63], нечіткий аналіз [64], інтелектуальний аналіз [65] та ін.

В зв'язку з тим, що виправлення недостовірних даних, які були вже внесені в БД і використані, викликає помітні труднощі, та в зв'язку з поширенням помилок, основним напрямком підвищення достовірності має бути орієнтація на процеси введення, зміни та перетворення даних [66].

Загальна модель оцінки достовірності даних, в системах прийняття рішень, повинна представляти дослідження потоків даних з вимірюванням ряду параметрів на етапах збору, введення, обробки, зберігання, передачі та подання інформації.

Модель повинна демонструвати можливі помилки в безлічі проміжних і кінцевих результатів. Водночас повинні бути враховані поширення і зміна помилок різних типів [67].

Управління рівнем достовірності інформації неможливе без попереднього встановлення зв'язку з джерелом інформації, контекстом і проведення її структурного аналізу [68]. Джерела даних, що містять послідовності подій, можуть бути змодельовані на системах кінцевого автомата. Правила узгодженості даних можуть бути виражені типовими методами і автоматично перевірені на даних, як до, так і після здійснення окремих дій [69]. Формальна процедура управління достовірністю даних на всіх етапах життєвого циклу інформації повинна змінювати показники достовірності в оцінки додаткової невизначеності, у зв'язку з недостатньою достовірністю даних [70].

Комплексний підхід до забезпечення достовірності даних повинен об'єднувати оцінку якості даних і архітектуру даних в єдину структуру з серією кроків, процедур, контрольних списків і інструментів і враховувати технології, процеси і проблеми користувачів [71].

Для оцінки сумісності, використовують умовні функціональні залежності [72]. Дослідники описали кілька підходів до роботи з втраченими даними, в першу чергу, намагаючись вивести значення або оцінки впливу втрачених даних за результатами. Проте, лише деякі з цих підходів визначають приховані структури (зміщення) в втрачених даних, тобто, визначають конкретні атрибути, які передбачають втрату значень даних. Знання специфічних систематичних моделей зміщення, при втраті даних, дасть змогу аналітикам точніше оцінити якість висновків з наборів даних із зниклими даними [73].

Отже, в сучасній літературі наведено досить широкий спектр методів оцінювання достовірності інформації. В багатьох публікаціях під достовірністю розуміється її якість, як характеристика можливості її

застосування у задачах прийняття рішень. Якість інформації є найбільш значимим фактором для прогнозування поведінки споживача. На теперішній час судження про ступінь достовірності інформації з боку користувачів базується переважно на когнітивних оцінках. Водночас окремі критерії користувачів щодо якості даних є достатньо різноманітними та віддзеркалюють об'єктивні особливості даних. На побутовому рівні довіра до інформації базується на двох рівнях: інституційному (домен походження, тип джерела, установа розповсюдження) та індивідуальному (ідентифікація автора, його ім'я, репутація). За таких умов один і той же ресурс може мати прийнятний рівень якості для однієї інформації і бути неприйнятним для іншої.

Основні методи оцінювання достовірності інформації поділяються на дві групи: евристичні та формальні. Загальна модель оцінки достовірності інформації інформаційних ресурсів має відбивати дослідження потоків з оцінюванням окремих критеріїв на етапах збирання, введення, обробки, зберігання, передачі та подання інформації. Розробка та застосування специфічних математичних моделей може допомогти особам, які приймають рішення, оцінювати достовірність інформації з урахуванням факторів можливого інформаційного впливу.

1.4. Аналіз протиріч та постановка наукового завдання

Темі достовірності інформації, традиційно, приділяється велика увага в теорії і практиці управління соціально-економічними системами. Останнім часом, даному напрямку приділяють увагу фахівці з інформаційної безпеки. Названі обставини спричинені значним збільшенням атак зловмисників

(конкурентів, злочинних елементів) на інформаційні ресурси підприємств і організацій, в умовах конкурентної боротьби.

Отже, множина «перешкод» - дестабілізуючих факторів, що мають вплив на достовірність і доступність інформації в сучасних інформаційних системах, не вписуються лише в класи відмов, збоїв і помилок апаратно-програмних засобів і операторів.

До того ж, достовірність і доступність інформації не може бути забезпечена простим включенням в компоненти системи відповідних елементів, процес підтримки достовірності і доступності повинен бути безперервним і керованим.

Таким чином, проблема забезпечення достовірності інформації виходить на новий рівень - рівень інформаційного протидії. У зв'язку з цим, необхідно переглянути концептуальні засади управління достовірністю і доступністю в інформаціоннотелекоммунікаціонних системах, розширити їх, наповнити новим змістом. Середовищем забезпечення достовірності і доступності інформації і об'єктом дослідження в даній роботі є організаційно-технічна система (ОТС) - взаємопов'язаний комплекс інформаційних ресурсів, засобів обчислювальної техніки, телекомунікацій, програмного забезпечення, персоналу і користувачів, що розглядається як єдине ціле при реалізації системних і прикладних інформаційних процесів, і призначена для забезпечення споживачів належним інформаційним обслуговуванням.

У численних роботах вітчизняних і зарубіжних дослідників, в роботах авторів згадуються такі особливості управління процесом, забезпечення достовірності інформації в ОТС:

- процес забезпечення достовірності інформації є погано формалізованим об'єктом управління, внаслідок перебування в умовах суттєвої невизначеності, джерелом якої є технічна і соціальна складові ОТС. Тут же відзначимо часту неможливість кількісного виміру значення вхідних і вихідних параметрів підсистем, високий їх взаємним вплив, що іноді

призводить до неможливості побудови аналітичних моделей приватних процедур управління процесом;

- наявність «людського фактора» призводить до того, що багато характеристик достовірності інформаційних ресурсів перестають бути строго визначеними, зв'язки між соціальною і технічної підсистемами є нечітко описаними, питання про кількість і склад вхідних даних, залишається відкритим, оскільки невідомо, що може вплинути на поведінку користувача, як елемента системи;

- якщо для зняття «невизначеності», при вивченні технічної підсистеми, використані класичні методи статистики, то для соціальної підсистеми вони є не придатними, оскільки невизначеність в даному випадку носить суб'єктивний характер.

Основне протиріччя, яке лежить в основі наукового дослідження полягає, з одного боку в тому, що інформація, яка добувається, передається та зберігається, не завжди може бути представлена у вигляді даних чи відомостей на машинних носіях у стандартизованому чи формалізованому вигляді, а, відтак потребує особливих підходів щодо її захисту від спотворення. З іншого боку, вплив інформаційного протиборства, який також є інформаційним, також не може бути представленим методами формальних теорій та числень, що унеможливлює його оцінювання під час оцінки достовірності інформації.

Отже, вирішенню підлягає актуальне наукове завдання щодо *розроблення методики оцінювання достовірності інформації в умовах інформаційного протиборства* для захисту інформаційних ресурсів організації та забезпечення інформаційної безпеки користувачів.

Підсумовуючи вищесказане, відзначимо, що управління процесом забезпечення достовірності інформації в ОТС потрібно розглядати, як складний інтелектуальний процес розв'язання проблем, який не може зводитися виключно до раціонального вибору. Для підтримки цього процесу, є доцільним використання когнітивного підходу до моделювання та

управління, оскільки він спрямований на розробку формальних моделей і методів, що підтримують інтелектуальний процес вирішення завдань управління, завдяки врахуванню в цих моделях і методах когнітивних можливостей людини.

Висновки до розділу 1

1. Інформаційний простір суспільства є результатом його еволюції і утворюється як сукупність інформації, інформаційної інфраструктури та суб'єктів, що здійснюють збір, формування, поширення і використання інформації. На сьогоднішній день, він дедалі частіше розглядається як сфера ведення інформаційної війни у технічному та психологічному доменах. Інформаційний простір є середовищем для здійснення процесу комунікації, який включає інформаційний ресурс, трансміттер, канал комунікації, процедури прийому сигналу та отримувача (реципієнта). На будь-який з цих елементів може чинитися вплив з боку зацікавлених осіб в рамках інформаційного протиборства.

2. Особливостями інформаційного простору, які впливають на процеси передачі інформації у ньому, є інформаційне протиборство, яке включає: вплив людського фактора, наявність конфліктів, багатовимірність, багатозвязність та самоорганізацію. Одним з визначальних – є вплив на інформацію інформаційної зброї, яка включає широкий клас прийомів і засобів інформаційного впливу – від дезінформації і пропаганди до засобів радіоелектронної боротьби. Інформаційна зброя реалізується через технічні засоби (віруси та інше шкідливе програмне забезпечення, APT-атаки та фізичний вплив на інформаційні системи) та засоби інформаційно-психологічного впливу: друковані матеріали, засоби масової інформації,

інтернет-ресурси, когнітивну зброю. Можливість впливу на інформацію реалізується на будь-якому з етапів її існування – від зародження (спостереження, опису, фіксації фактів) до моменту доставки до кінцевого споживача.

3. В сучасній літературі наведено досить широкий спектр методів оцінювання достовірності інформації. В багатьох публікаціях під достовірністю розуміється її якість, як характеристика можливості її застосування у задачах прийняття рішень. Якість інформації є найбільш значимим фактором для прогнозування поведінки споживача. На теперішній час судження про ступінь достовірності інформації з боку користувачів базується переважно на когнітивних оцінках. Водночас окремі критерії користувачів щодо якості даних є достатньо різноманітними та віддзеркалюють об'єктивні особливості даних. На побутовому рівні довіра до інформації базується на двох рівнях: інституційному (домен походження, тип джерела, установа розповсюдження) та індивідуальному (ідентифікація автора, його ім'я, репутація). За таких умов один і той же ресурс може мати прийнятний рівень якості для однієї інформації і бути неприйнятним для іншої.

4. Основні методи оцінювання достовірності інформації поділяються на дві групи: евристичні та формальні. Загальна модель оцінки достовірності інформації інформаційних ресурсів має відбивати дослідження потоків з оцінюванням окремих критеріїв на етапах збирання, введення, обробки, зберігання, передачі та подання інформації. Розробка та застосування специфічних математичних моделей може допомогти особам, які приймають рішення, оцінювати достовірність інформації з урахуванням факторів можливого інформаційного впливу.

5. Основне протиріччя, яке лежить в основі наукового дослідження полягає, з одного боку в тому, що інформація, яка добувається, передається та зберігається, не завжди може бути представлена у вигляді даних чи відомостей

на машинних носіях у стандартизованому чи формалізованому вигляді, а, відтак потребує особливих підходів щодо її захисту від спотворення. З іншого боку, вплив інформаційного протиборства, який також є інформаційним, також не може бути представленим методами формальних теорій та числень, що унеможливлює його оцінювання під час оцінки достовірності інформації.

6. Таким чином, вирішенню підлягає актуальне наукове завдання щодо *розроблення методики оцінювання достовірності інформації в умовах інформаційного протиборства* для захисту інформаційних ресурсів організації та забезпечення інформаційної безпеки користувачів.

РОЗДІЛ 2.
РОЗРОБКА МОДЕЛІ ДОСТОВІРНОСТІ ІНФОРМАЦІЇ В УМОВАХ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА

2.1. Розробка базової моделі інформаційного протиборства

У теперішній час національна безпека України все більш залежить від ступеня її інформаційної безпеки. Традиційно, питання інформаційної безпеки відносяться до гуманітарної (інформаційно-психологічної) сфери і тому є складними для моделювання. Разом з тим, впровадження у дослідження цих питань математичних методів здатне суттєво збагатити науково-методичний апарат соціологічного знання та соціальної психології.

У контексті розгляду активних інформаційних дій актуальним є питання розроблення математичних моделей, які описують процеси інформаційної війни та інформаційного протиборства. Це, у свою чергу, дозволить якісно вивчити характер процесів, які розглядаються, а також дає можливість ставити та вирішувати завдання щодо знаходження оптимальних способів їх організації.

У загальному вигляді зазначені процеси є нелінійними і тому допускають неочевидні режими їх розвитку. Водночас, навіть у найпростіших випадках, аналіз математичних моделей та результатів розрахунків дають змогу визначати ключові характеристики, управління якими стимулюватиме напрямок розвитку ситуації у необхідному напрямку.

Базова модель інформаційного впливу. Нехай існує група взаємодіючих індивідів чисельністю N_0. Передбачається, що неохоплений інформацією індивід може одержати її від ЗМІ, або шляхом міжособової

комунікації від інформованого раніше індивіда (прихильника). Чисельність прихильників у момент часу t позначимо через $X(t)$. Інтенсивність розповсюдження інформації цими способами описується позитивними параметрами α і β відповідно, причому ці параметри є незалежними від часу. Також необхідно відзначити, що швидкість розповсюдження інформації через міжособистісну комунікацію при цьому також пропорційна числу вже охоплених індивідів. Передбачається, що швидкість розповсюдження інформації (число охоплених індивідів за одиницю часу) складається зі швидкостей розповсюдження інформації кожним з вищезгаданих способів. Ця швидкість є пропорційною числу ще неохоплених індивідів, тобто $N_0 - X(t)$.

Для розповсюдження інформації через ЗМІ будемо вважати, що соціум знаходиться у свого роду “всеосяжному нелокальному інформаційному полі”, тобто будь-який з ще не завербованих членів товариства завжди має можливість одержати та сприйняти цю інформацію. Відмітимо також, що хоча міжособистісна комунікація має локальний характер (від людини до людини), але швидкість вербування, як і у першому випадку, знову ж таки є пропорційною числу ще не завербованих членів товариства $N_0 - X(t)$.

Загальна швидкість зміни числа прихильників $X(t)$ – число завербованих у одиницю часу, складається з швидкості розповсюдження інформації через ЗМІ та через міжособистісну комунікацію

$$\frac{\partial X(t)}{\partial t} = (\alpha + \beta X)(N_0 - X), X(0) = 0, \tag{2.1}$$

де $N(t)$ – кількість прихильників в момент часу *t*. Рішення задачі (2.1) має вигляд

$$X = N_0 \frac{\alpha\, exp[\alpha + \beta N_0 t] - \alpha}{\alpha\, exp[\alpha + \beta N_0 t] + \beta N_0}, \tag{2.2}$$

Модель (2.2) є базовою і у подальшому буде використовуватись для опису явищ поширення інформації. Одним з основних питань, які вирішуються за допомогою моделей поширення інформації, є питання щодо умов, за яких швидкість росту кількості прихильників досягає максимуму (явище максимального ажіотажу).

У [74] показано, що максимум ажіотажу досягається при значенні чисельності прихильників, яке дорівнює

$$X_g = \frac{1}{2\left(N_0 - \frac{\alpha}{\beta}\right)}, \tag{2.3}$$

Якщо $N_0 \le \frac{\alpha}{\beta}$, то швидкість росту кількості прихильників максимальна в початковий момент і спадає з часом.

Також цікавим є питання про те, як буде змінюватись швидкість росту кількості прихильників при інтенсивності розповсюдження інформації через слухи, яка спадає з ростом *X*. Розглянемо більш загальну, ніж (2.1) модель, у якій передача інформації через слухи описується степеневим виразом

$$\frac{\partial X}{\partial t} = \left(\alpha + \beta X^{\mu}\right)\left(N_0 - X\right), X(0) = 0, \tag{2.4}$$

Випадки при $\mu = 2, \mu = \frac{1}{2}$ розглянуті у [75]. Щоб визначити наявність ажіотажу необхідно визначити $\frac{\partial^2 X}{\partial t^2}$:

$$\frac{\partial^2 X}{\partial t^2} = -\beta\mu \frac{\partial X}{\partial t}\left[X^{\mu-2}\left(\frac{\mu+1}{\mu} X - N_0 \right) + \frac{\alpha}{\beta\mu} \right], \qquad (2.5)$$

Очевидно, що при $\mu < 0$ маємо $\frac{\partial^2 X}{\partial t^2} < 0$, тобто швидкість росту кількості прихильників $\frac{\partial X}{\partial t}$ з часом зменшується. Деякі інші підходи до моделювання розповсюдження інформації в соціумі запропоновані у роботах [76].

Базова модель інформаційного протиборства. Нехай тепер, на відміну від (2.1), існує соціальна спільність чисельністю N_0, яка потенційно може перебувати під впливом не одного, а двох різнорідних між собою за змістом інформаційних потоків (як правило, інформація I_1 та I_2 – діаметрально протилежні). Нехай у момент часу $t = 0$ два джерела різної інформації одночасно починають її транслювати, у результаті чого обидва інформаційних потоки розповсюджуються серед суспільства.

Оскільки I_1 та I_2 не тотожні один одному, то даний процес розглядається як інформаційна протидія (конкуренція). Модель описує динаміку його розвитку з часом, тобто залежні від часу *t* величини $X(t)$ і $Y(t)$ числа "прихильників", які сприйняли інформацію, що розповсюджується джерелами "1" і "2", а також визначають її кінцевий результат – переможця чи переможеного. Переможцем вважається той, хто до моменту повного охоплення спільності обома видами інформації зумів розповсюдити свою інформацію серед більшої, ніж суперник, кількості членів групи, тобто величиною, більшою, ніж $\frac{N_0}{2}$.

У цій моделі передбачається, що індивід, який одержав інформацію від одного з джерел, є закритим для іншого, тобто перевербування виключається.

Також робиться припущення про те, що кожне з джерел характеризується своїми значеннями величин, які описують інтенсивність розповсюдження інформації (α_1,β_1 для першого і α_2,β_2 для другого джерела інформації). У цій моделі швидкість розповсюдження шляхом міжособистісної комунікації для кожного із джерел є пропорційною числу індивідів, охоплених цим же джерелом, а число неохоплених індивідів дорівнює величині $N_0 - X(t) - Y(t)$, де $X(t)$ – число індивідів, охоплених першим джерелом, а $Y(t)$ – число індивідів, охоплених другим джерелом. Таким чином базова модель інформаційної протиборства буде

$$\frac{\partial X}{\partial t} = (\alpha_1 + \beta_1 X)(N_0 - X - Y), X(0) = 0, \tag{2.6}$$

$$\frac{\partial Y}{\partial t} = (\alpha_2 + \beta_2 X)(N_0 - X - Y), Y(0) = 0 \tag{2.7}$$

Важливим моментом для розгляду (2.6) – (2.7) є також питання щодо "переможця" та "переможеного", що може бути інтерпретовано, як яка сторона змогла розповсюдити свою інформацію серед більшого, ніж суперник, числа членів спільності до моменту повного охоплення соціуму обома видами інформації.

У роботі [74] на основі аналізу стаціонарного рішення системи (2.6) – (2.7) було одержано необхідні і достатні умови "перемоги" I_1 над I_2, тобто виконано нерівності $X^f > Y^f$, де X^f, Y^f – значення чисельностей $X(t)$, $Y(t)$ у момент закінчення процесу, коли $X^f + Y^f = N_0$. Воно матиме вигляд

$$\frac{\beta_1}{ln\left(1 + \frac{\beta_1 N_0}{2\alpha_1}\right)} > \frac{\beta_2}{ln\left(1 + \frac{\beta_2 N_0}{2\alpha_2}\right)}, \tag{2.8}$$

Нерівність протилежного знаку буде означати перемогу I_2 над I_1, а рівність – нічию. Необхідно також відзначити, що за ненульових значень початкової кількості прихильників інформації I_1 та I_2 на кінцевий результат будуть впливати також і значення $X(0)$, $Y(0)$.

Для більш складного випадку модель (2.6) – (2.7) може бути узагальнена на ситуацію протиборства не двох, а більшої кількості видів інформації. У цьому випадку вона являтиме собою систему M нелінійних звичайних диференційних рівнянь:

$$\frac{\partial N_i}{\partial t} = \left(\alpha_i + \beta_i N_i\right)\left(N_0 - \sum_{i=1}^{M} N_i\right), N_i(0) = 0, i = \overline{1,M}, \qquad (2.9)$$

Таким чином, у контексті розгляду активних інформаційних дій актуальним є питання розроблення математичних моделей, які описують процеси інформаційної війни та інформаційного протиборства. Базова модель інформаційного впливу базується на динаміці зміни числа прихильників інформаційного повідомлення – тобто тих, хто сприймає інформацію через визначений канал комунікації. На відміну від моделі інформаційного впливу, модель інформаційного протиборства передбачає наявність двох конфліктуючих інформаційних потоків, які розповсюджуються серед суспільства. Побудова моделей у вигляді диференційних рівнянь дає можливість досліджувати динаміку розповсюдження інформації. При цьому визначення “переможця” чи “переможеного” залежить від того, яка сторона змогла розповсюдити свою інформацію серед більшого, ніж суперник, числа членів спільності до моменту повного охоплення соціуму обома видами інформації.

2.2. Урахування додаткових факторів впливу у моделі інформаційного протиборства

Розповсюдження інформації з урахуванням забування. З метою урахування додаткових факторів загальна модель (2.6) – (2.7) може бути розширена за рахунок введення складових, які відображають процеси: забування інформації індивідами, неповного охоплення соціуму засобами масової інформації, багатократного засвоєння та забування інформації.

Модель, яка враховує забування інформації індивідами (перехід прихильників до множини неохоплених інформацією) буде мати вигляд [77]:

$$\frac{\partial X(t)}{\partial t} = (\alpha + \beta X)(N_0 - X) - \gamma X, X(0) = X_0, \qquad (2.10)$$

де $\gamma > 0$ – інтенсивність забування інформації індивідами.

Відшукаємо стаціонарне рішення рівняння (2.10), для чого необхідно вирішити рівняння $(\alpha + \beta X)(N_0 - X) - \gamma X = 0$. Це рівняння, за будь-яких додатних значень $\alpha, \beta, \gamma, N_0 > 0$ має два корені, лише один з яких є додатним. Таким чином стаціонарне рішення завжди існує і дорівнює

$$X^s = \frac{-\gamma - \alpha + \beta N_0 + \sqrt{(\gamma + \alpha - \beta)N_0^2 + 4\alpha\beta N_0}}{2\beta}, \qquad (2.11)$$

Аналізуючи знаки похідних в околиці стаціонарного рішення, одержимо, що дане рішення є стійким.

Дослідимо залежність стаціонарного рішення від параметрів.

Побудуємо графік функції $X^s(\gamma)$. За будь-яких додатних значень параметрів перша похідна від'ємна, друга додатна, $X^s(0)=N_0$, $\lim\limits_{\gamma\to\infty} X^s(\gamma)=0$. Графік функції $X^s(\gamma)$ має вигляд, наведений на рис. 2.1. З графіка слідує, що у достатньо широкому діапазоні γ залежність $X^s(\gamma)$ має майже лінійний характер.

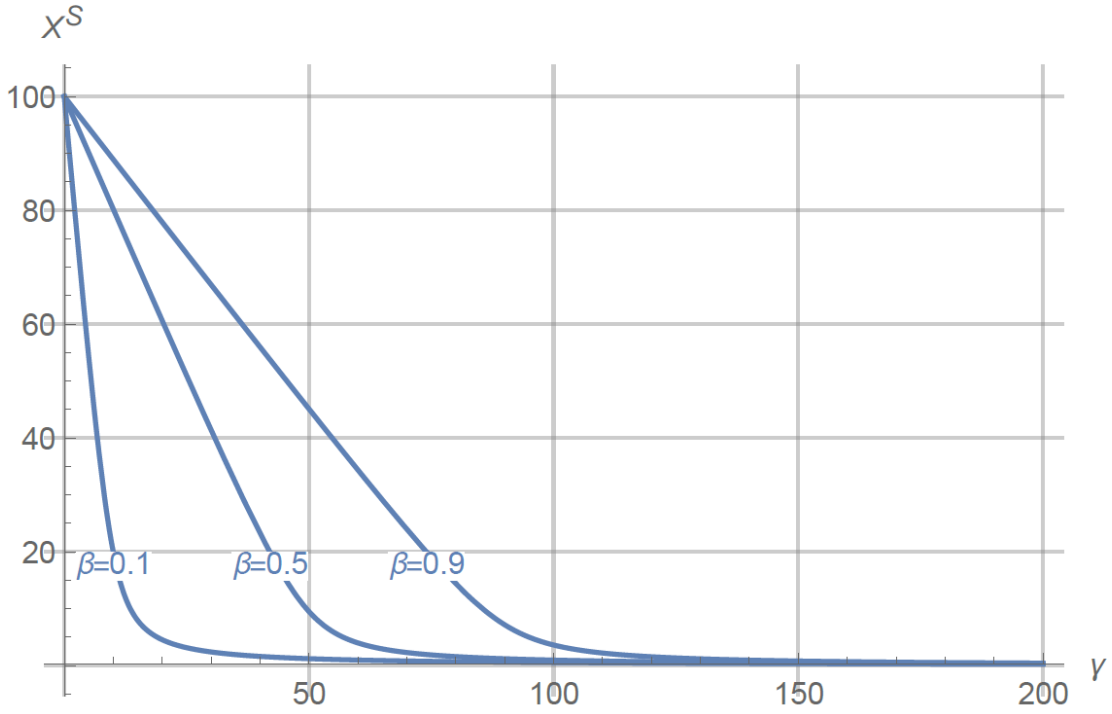

Рис. 2.1. Графік залежності $X^s(\gamma)$

Модель (2.10) дає змогу вирішувати широке коло задач. Зокрема, часто необхідним є визначення необхідних параметрів джерела інформації за заданої частки охоплення усього населення μ. При цьому передбачається, що джерело інформації може впливати лише на інтенсивність розповсюдження інформації через ЗМІ, тобто на параметр α і йому відомі значення інших параметрів. Тобто, необхідно вирішити наступну задачу: знайти α таке, що $X^s = \mu N_0$. Вирішуючи цю задачу, одержимо:

$$\alpha^* = \frac{\mu(\gamma - \beta N_0(1-\mu))}{1-\mu}, \qquad (2.12)$$

Аналізуючи функцію $X(t)$ можна побачити, що, у залежності від початкових умов, графік функції буде мати вигляд кривої 1, 2, або 3 (рис. 2.2).

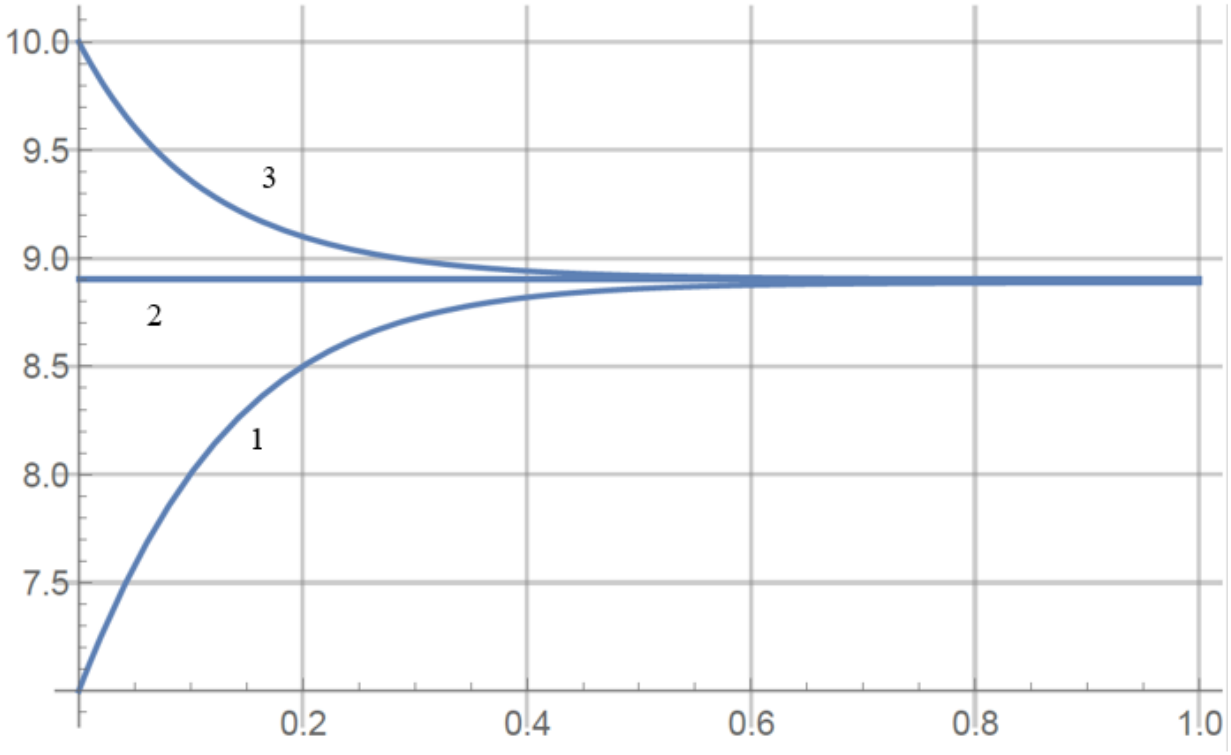

Рис. 2.2. Графіки чисельності прихильників $X(t)$ при різних початкових умовах

Якщо $X(0) < X^s$, то перша похідна функції $X(t)$ додана, а друга від'ємна, графік функції має вигляд 1; якщо $X(0) = X^s$, обидві похідні дорівнюють нулю, графік функції має вид 2; якщо $X(0) > X^s$, то перша похідна від'ємна, друга додатна, графік має вид 3.

Розглянемо детальніше випадок нульової початкової умови, тобто $X(0) = 0$. У цьому випадку аналіз другої похідної функції $X(t)$ показує, що

швидкість вербування зменшується з часом, якщо $N_0 < \frac{\alpha+\gamma}{\beta}$, є максимально можливою у початковий момент часу, а потім зменшується, при $N_0 = \frac{\alpha+\gamma}{\beta}$ спочатку збільшується, потім досягає максимуму у точці максимального ажіотажу, після чого зменшується, якщо $N_0 > \frac{\alpha+\gamma}{\beta}$.

Аналітичне рішення рівняння (2.10) є достатньо громіздким. Разом з тим представляє цікавість випадок сильної пропаганди ($\alpha >> N_0\beta$). При цьому припущенні, як показано у [78] стає можливим застосування методів теорії сингулярних збуджень. У відповідності з методом граничних функцій невідому функцію $X(t)$ можна подати у вигляді суми регулярного і граничного рядів за малим параметром $\varepsilon = \frac{1}{\alpha}$:

$$X(t) = \bar{X}^0(t) + \Pi_0 X(\tau) + \varepsilon\left(\bar{X}^1(t) + \Pi_1 X(\tau)\right) + o(\varepsilon), \qquad (2.13)$$

де $\tau = \frac{t}{\varepsilon}$,

$\Pi_0 X(\tau)$, $\Pi_1 X(\tau)$ – граничні функції такі, що $\lim\limits_{\tau\to\infty} \Pi_i X(\tau) = 0, i = 0,1$.

Підставивши розкладання (2.13) у вираз (2.10) та прирівнявши коефіцієнти при відповідних степенях ε, одержимо рівняння для нульового та першого наближень функції $X(t)$. Вирішуючи їх та підставляючи знайдені вирази у (2.13) одержимо перше наближення рішення цього рівняння

$$X(t) = 1 - e^{-\tau} + \varepsilon\left[\beta N_0 - \gamma + e^{-2\tau}\left(\beta N_0 - 2\beta e^{\tau} N_0 + \beta e^{\tau} N_0 \tau + \gamma e^{\tau} - \gamma \tau e^{\tau}\right)\right], \quad (2.14)$$

Розповсюдження інформації між відокремленими групами. Запропоновані моделі дозволяють розширити їх за рахунок включення передбачення про поділ соціуму на дві групи населення, кожна з яких характеризується своїми значеннями параметрів α і β. Позначимо чисельність першої групи населення через N_1, а другої через N_2. Тоді одержимо наступну систему рівнянь:

$$\frac{\partial X_1}{\partial t} = \left(\alpha_1 + \beta_1\left(X_1 + X_2\right)\right)\left(N_1 - X_1\right), \tag{2.15}$$

$$\frac{\partial X_2}{\partial t} = \left(\alpha_2 + \beta_2\left(X_1 + X_2\right)\right)\left(N_2 - X_2\right) \tag{2.16}$$

Побудуємо фазовий портрет системи (2.15) – (2.16). У загальному випадку система має три положення рівноваги, лише одне з яких (N_1, N_2) знаходиться у першій чверті координатної площини. Лінеаризувавши систему у околиці положення рівноваги можна одержати, що положення рівноваги – це стійкий вузол.

Лінеаризована система (2.15) – (2.16) в околиці положення рівноваги (N_1, N_2) після заміни змінних $\xi = X_1 - N_1$, $\eta = X_2 - N_2$ має вигляд:

$$\frac{\partial \xi}{\partial t} = \left(\alpha_1 + \beta_1\left(N_1 + N_2\right)\right)\left(-\xi\right), \tag{2.17}$$

$$\frac{\partial \eta}{\partial t} = \left(\alpha_2 + \beta_2\left(N_1 + N_2\right)\right)\left(-\eta\right) \tag{2.18}$$

Власні значення матриці

$$\begin{pmatrix} -\left(\alpha_1 + \beta_1\left(N_1 + N_2\right)\right) & 0 \\ 0 & -\left(\alpha_2 + \beta_2\left(N_1 + N_2\right)\right) \end{pmatrix}$$

мають значення $-(\alpha_1+\beta_1(N_1+N_2))$ та $-(\alpha_2+\beta_2(N_1+N_2))$. Обидва вони від'ємні, тому, положення рівноваги – стійкий вузол.

Фазовий портрет зображено на рис. 2.3.

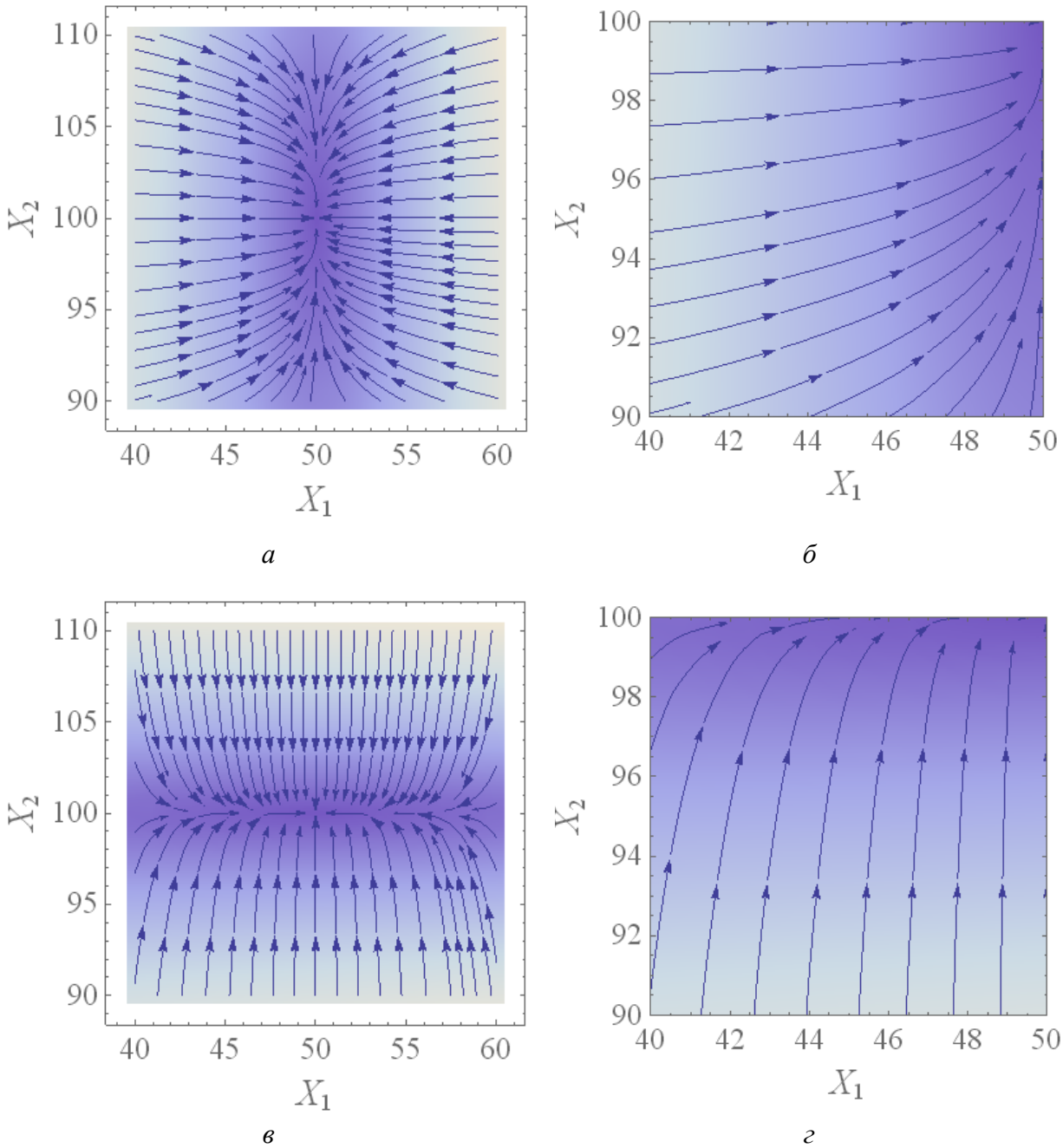

Рис. 2.3. Фазовий портрет системи (2.15) – (2.16). Рисунки а, в – загальний вигляд. Область змінних виділена на рисунках б, г. Значення параметрів на рисунках а, б: N1 = 50; N2 = 100, = 0,2; = 0,6; = 0,8; = 0,2. Значення параметрів на рисунках в, г: N1 = 50; N2 = 100, = 0,6; = 0,4; = 0,1; = 0,9

Вид фазового портрета залежить від співвідношення $-(\alpha_1+\beta_1(N_1+N_2))$ та $-(\alpha_2+\beta_2(N_1+N_2))$. Якщо $|-\alpha_1-\beta_1(N_1+N_2)|>|-\alpha_2-\beta_2(N_1+N_2)|$, то фазовий портрет має вигляд, зображений на рис. 2.3а, 2.3б якщо $|-\alpha_1-\beta_1(N_1+N_2)|<|-\alpha_2-\beta_2(N_1+N_2)|$, то фазовий портрет має вигляд, зображений на рис. 2.3в, 2.3г.

Розглянемо тепер випадок двох груп населення, які відрізняються тим, що вони більше довіряють індивідам зі своєї групи, ніж індивідам з чужої групи. Тоді модель описується наступною системою рівнянь:

$$\frac{\partial X_1}{\partial t}=(\alpha_1+\beta_1X_1+\beta_2X_2)(N_1-X_1), \tag{2.19}$$

$$\frac{\partial X_2}{\partial t}=(\alpha_2+\beta_2X_1+\beta_1X_2)(N_2-X_2) \tag{2.20}$$

$$\beta_1>\beta_2 \tag{2.21}$$

Система (2.19) – (2.21) також має три положення рівноваги, одне з яких (N_1,N_2) знаходиться у першій чверті.

Лінеаризована система (2.19) – (2.21) в околиці положення рівноваги (N_1,N_2) після заміни змінних $\xi=X_1-N_1$, $\eta=X_2-N_2$ має вигляд:

$$\frac{\partial \xi}{\partial t}=(\alpha_1+\beta_1N_1+\beta_2N_2)(-\xi), \tag{2.22}$$

$$\frac{\partial \eta}{\partial t}=(\alpha_2+\beta_2N_1+\beta_1N_2)(-\eta) \tag{2.23}$$

Власні значення матриці $\begin{pmatrix} -(\alpha_1+\beta_1 N_1+\beta_2 N_2) & 0 \\ 0 & -(\alpha_2+\beta_2 N_1+\beta_1 N_2) \end{pmatrix}$ дорівнюють $-(\alpha_1+\beta_1 N_1+\beta_2 N_2)$ та $-(\alpha_2+\beta_2 N_1+\beta_1 N_2)$. Обидва значення від'ємні, що означає, що положення рівноваги – стійкий вузол.

Вигляд фазового портрета залежить від співвідношення $-(\alpha_1+\beta_1 N_1+\beta_2 N_2)$ та $-(\alpha_2+\beta_2 N_1+\beta_1 N_2)$. Якщо $|-(\alpha_1+\beta_1 N_1+\beta_2 N_2)|>|-(\alpha_2+\beta_2 N_1+\beta_1 N_2)|$, то фазовий портрет має вигляд, зображений на рис. 2.3а, якщо $|-(\alpha_1+\beta_1 N_1+\beta_2 N_2)|<|-(\alpha_2+\beta_2 N_1+\beta_1 N_2)|$, то фазовий портрет має вигляд, зображений на рис. 2.3б.

Урахування процесів засвоєння інформації. Практика свідчить, що інформаційний вплив буде результативним, якщо він є не однократним, а проводиться у вигляді кампанії. У рамках цього варіанту моделі передбачається, що індивід долучається до числа прихильників за два кроки. Будучи охопленим з першого разу він стає *предприхильником*. Це, зокрема, означає, що він ще не розповсюджує інформацію далі. Предприхильник одержує і засвоює інформацію за тими ж правилами, що і неохоплений нею член групи.

Позначимо через $x(t)$ чисельність предприхильників. Прихильники рекрутуються з предприхильників, тому $\frac{\partial X}{\partial t}=x(\alpha+\beta X)$.

Оскільки прихильники рекрутуються з неохоплених індивідів, чисельність яких в момент часу t складає $N_0-X(t)-x(t)$, маємо рівняння динаміки чисельності предприхильників $\frac{\partial x}{\partial t}=(N_0-X-2x)(\alpha+\beta X)$.

Узагальнення моделі інформаційного протиборства. Вище було розглянуто три додаткових фактора розповсюдження інформації: неповне охоплення соціуму засобами масової інформації, двокрокове засвоєння

інформації та забування. Загальна модель інформаційної протидії, яка враховує усі ці фактори матиме вигляд:

$$\frac{\partial X_1}{\partial t} = (\alpha_1 + \beta_1(X_1 + X_2)) - \gamma_1 X_1 \quad (2.24)$$

$$\frac{\partial X_2}{\partial t} = \beta_1 x_2 (X_1 + X_2) - \gamma_1 X_2 \quad (2.25)$$

$$\frac{\partial Y_1}{\partial t} = y_1(\alpha_2 + \beta_2(Y_1 + Y_2)) - \gamma_2 Y_1 \quad (2.26)$$

$$\frac{\partial Y_2}{\partial t} = \beta_2 y_2 (Y_1 + Y_2) - \gamma_2 Y_2 \quad (2.27)$$

$$\frac{\partial x_1}{\partial t} = (\alpha_1 + \beta_1(X_1 + X_2))(N_1 - X_1 - Y_1 - 2x_1 - y_1) + \gamma_1 X_1 - \delta_1 x_1 \quad (2.28)$$

$$\frac{\partial x_2}{\partial t} = \beta_1(X_1 + X_2)(N_2 - X_2 - Y_2 - 2x_2 - y_2) + \gamma_1 X_2 - \delta_1 x_2 \quad (2.29)$$

$$\frac{\partial y_1}{\partial t} = (\alpha_2 + \beta_2(Y_1 + Y_2))(N_1 - X_1 - Y_1 - 2y_1) + \gamma_2 Y_1 - \delta_2 y_1 \quad (2.30)$$

$$\frac{\partial y_2}{\partial t} = \beta_2(Y_1 + Y_2)(N_2 - X_2 - Y_2 - x_2 - 2y_2) + \gamma_2 Y_2 - \delta_2 y_2 \quad (2.31)$$

$$X_1(0) = X_2(0) = Y_1(0) = Y_2(0) = x_1(0) = x_2(0) = y_1(0) = y_2(0) = 0 \quad (2.32)$$

У зазначеній системі x_1, x_2 – число предприхильників з відповідно першої та другої груп, охоплених джерелом 1; y_1, y_2 – число предприхильників з відповідно першої та другої груп, охоплених джерелом 2; X_1, X_2 – число прихильників з відповідно першої та другої груп, охоплених джерелом 1; Y_1, Y_2 – число прихильників з відповідно першої та другої груп, охоплених джерелом 2; α_1, α_2 – параметри, які характеризують інтенсивність розповсюдження інформації відповідно першим та другим джерелом через ЗМІ; β_1, β_2 – параметри, які характеризують інтенсивність розповсюдження

інформації відповідно першим та другим джерелом через міжособистісну комунікацію; γ_1 , γ_2 – параметри, які характеризують забування прихильниками, охопленими відповідно першим та другим джерелом; δ_1, δ_2 – параметри, які характеризують забування предприхильниками, охопленими відповідно першим та другим джерелом; N_1 , N_2 – чисельність першої та другої груп.

Для дослідження наведених моделей можна застосувати чисельні методи. Особливу увагу виділено випадку, коли одна зі сторін володіє більш сильною пропагандою в ЗМІ, а інша – більш «вірусну» інформацію, тобто $\alpha_1 > \alpha_2,\ \beta_1 < \beta_2$.

Результати числових експериментів демонструють, що для кожної з груп динаміка в загальному, має вигляд: спочатку збільшується та досягає максимума кількість пред-прихильників, після вона зменшується, при цьому відбувається ріст кількості прихильників. На рисунках 2.4 - 2.5 зображена динаміка кількості прихильників і пред-прихильників з обох експериментальних груп з наступними значеннями параметрів:

$N_1 = 50,\ N_2 = 100,\ \gamma_1 = 0{,}01,\ \gamma_2 = 0{,}3,\ \delta_1 = 0{,}1, \delta_2 = 0{,}02, \alpha_1 = 0{,}13,\ \alpha_2 = 0{,}06, \beta_1 = 0{,}04, \beta_2 = 0{,}1$

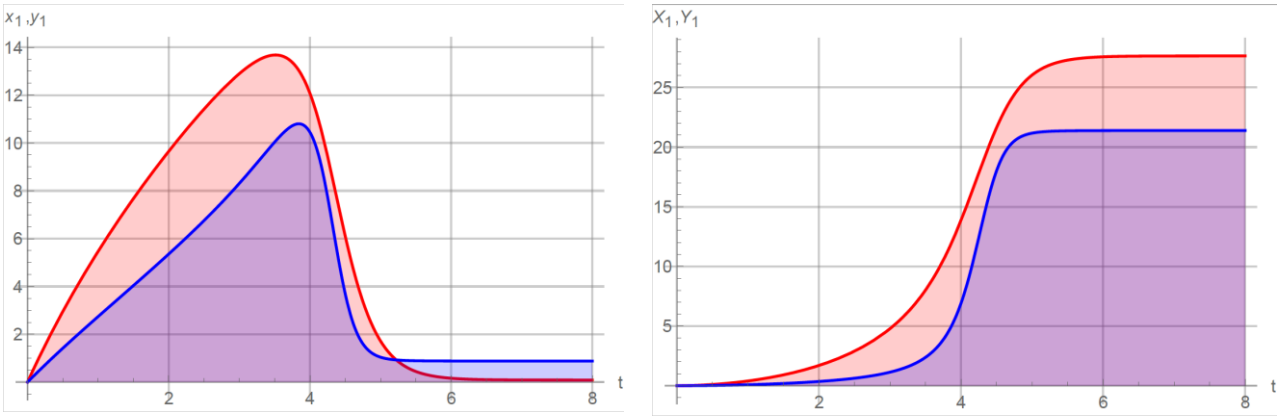

Рис. 2.4. Динаміка кількості прихильників та пред-прихильників з першої групи.

Синя лінія – x(t) та X(t), малинова лінія – y(t) та Y(t)

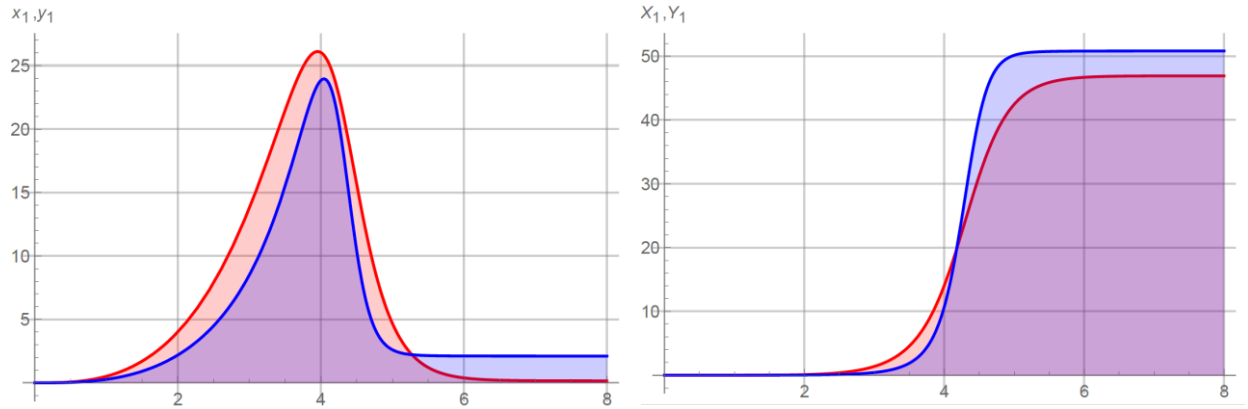

Рис. 2.5. Динаміка кількості прихильників та пред-прихильників з другої групи.

Синя лінія – x(t) та X(t), малинова лінія – y(t) та Y(t)

Рис. 2.4 – 2.5 зображають, що більшість членів першої групи (індивідуми, які користувались ЗМІ) охоплені першим джерелом ($X_1(t) > Y_1(t)$ при досить великих значеннях t), а більшість членів другої групи (ті, що не користувались ЗМІ) – другим джерелом ($X_2(t) < Y_2(t)$ при досить великих значеннях t). Якщо в першій групі перевага першого джерела, майже не помітна, то в другій группі кількісна різниця між тими хто захоплюється першим джерелом і тими хто довіряє другому, набагато більша. Ця різниця утворюється за рахунок того, що «вірусність» інформації другого джерела має великий вплив на обидві групи (тому що індивіди з різних груп спілкуються між собою), а перше джерело в той же час має значимість лише для першої групи. У випадку зростання значення коефіцієнтів α_1 і β_2, ми будемо спостерігати абсолютну владу другого джерела над всією другою групою, та одночасно з цим більшу перевагу мають люди першої групи, які захоплюються першим джерелом. При цьому збільшення коефіцієнтів забуття інформації, призводить до зміщення базового розподілу на користь другого джерела. Це відбувається по причині того, що індивіди «інформаційного забуття» мають більшу схильність до вербування другим джерелом, ніж першим.

Отже, запропонована базова модель інформаційного впливу може бути розширена за рахунок введення складових, які відображають процеси: забування інформації індивідами, неповного охоплення соціуму засобами масової інформації, багатократного засвоєння та забування інформації. Крім того, можливе також розширення моделей за рахунок включення передбачення про поділ соціуму на дві групи населення, кожна з яких характеризується своїми значеннями додаткових параметрів (інтенсивність розповсюдження інформації через ЗМІ та під час особистої комунікації). Подальшим удосконаленням моделі є урахування процесів засвоєння інформації, які передбачають багатократне проведення інформаційних кампаній. Отже, результуюча узагальнена модель інформаційної протидії включає систему диференційних рівнянь, які описують зміну кількості прихильників інфомаційних повідомлень, що належать до різних груп у залежності від параметрів груп та частоти появи повідомлень.

2.3. Обгрунтування основних компонентів моделі достовірності інформації

Розглянемо компоненти концептуальної моделі процесу забезпечення достовірності інформації (ЗДІ) на першому (найвищому, найбільш абстрактному) рівні декомпозиції: інформаційні ресурси (ІР), джерела інформації (ДІ), фактори інформаційного протиборства (ФІП), джерела факторів інформаційного протиборства (загроз достовірності), цілі зловмисників, функції, методи та засоби забезпечення достовірності, показники достовірності.

При цьому врахуванню також підлягають особливості інформаційного простору, які впливають на процес забезпечення достовірності інформації. У роботі пропонується концепція управління процесами забезпечення достовірності інформаційних ресурсів (ІР) в ІП, що відрізняється урахуванням:

- факторів інформаційного протиборства, що здійснюють вплив на достовірність інформації в інформаційному просторі;
- моніторингу і динамічного визначення рівня достовірності джерел інформації.

Інформаційні ресурси та джерела інформації. Інформація – об’єктивна категорія, яка формує додаткові знання (згідно визначення Шеннона) про якийсь об’єкт чи явище. Інформація проявляється в повідомленнях ДІ, де повідомлення – вибрана частина інформації, яка містить закінчений сенс. Інформаційні повідомлення, як об’єктивна реальність, абсолютно завжди достовірні.

В ІП циркулюють данні – оброблені повідомлення, які представленні в формалізованому вигляді (наприклад, у вигляді цифрового коду), який придатний для передачі, перетворення і представлення в деякому інформаційному процесі для вирішення задач індивідів. Індивід, як правило, не є безпосереднім спостерігачем об’єкту чи явища, а повинен задовольнятися даними про об’єкти, які отримує від деякого ДІ, який є або безпосереднім «спостерігачем» обєкта або явища, або транслює данні, які отримує з інших джерел, в кращому випадку, з першоджерел. При цьому ДІ можуть перекривати один одного і формувати суперечливу інформацію. Конфлікти значень в суперечливих джерелах часто систематичні і викликані властивостями різних джерел [79].

Інформаційні повідомлення до часу «приховані» в ДІ, проявляються в вигляді даних в момент ініціювання задач індивідів шляхом фіксації на фізичних носіях чи при передачі по фізичному каналу зв’язку в ІП. Ці данні

зберігаються, піддаються перетворенню, представляються індивідам, які за допомогою даних процесів обробки приймають інформаційні повідомлення. Далі повідомлення «розчиняються» в споживачах (користувачів).

Данні, що отримуються при кодуванні повідомлень, можуть виявитися правдивими (правдоподібні, неправдоподібні), повні (недостатньо повні для задач користувачів), актуальні (застарівші для задачі, що вирішуються) і т.д. Ступінь довіри до таких даних визначається їх семантичною і «тимчасовою» спотвореністю.

Зафіксовану сукупність даних в ІП будемо називати інформаційним ресурсом (ІР). Державні інформаційні ресурси – це результати інтелектуальної та практичної діяльності, що сформовані в усіх сферах життєдіяльності людини, суспільства і держави, зафіксовані і систематизовані на відповідних матеріальних носіях інформації, як окремі документи і масиви документів, банки і бази даних та знань, усі види архівів і бібліотек, музейні фонди, інформаційні ресурси, які обробляються й передаються у інформаційних системах державного і/або загального призначення, інші ресурси, що містять дані, відомості і знання, які є об’єктом права власності держави незалежно від форми власності на час їх створення і мають споживчу цінність, а також такі, що призначені для розвитку і задоволення потреб громадян, суспільства, держави та підлягають захисту згідно визначеної політики безпеки й чинного законодавства [80].

Державні інформаційні ресурси можуть бути розділені на дві групи:

1) інформаційні ресурси, призначені для вирішення завдань конкретного органу управління певної ланки;

2) інформаційні ресурси, орієнтовані на зовнішнього користувача. Останні формуються інформаційно-аналітичними структурами. Якщо вони мають загальне методичне керівництво, схожі завдання, які вирішуються на основі єдиних нормативних документів, то вони можуть бути названі державними інформаційними системами. До державних інформаційних

ресурсів висуваються вимоги щодо актуальності та достовірності наведених у них даних; вичерпної повноти інформаційних джерел; компактності викладу; оперативності пошуку. Державні інформаційні ресурси мають типову структуру: обов'язкову – основну частину і вихідні дані; факультативну – довідково-бібліографічний апарат і додаткову інформацію [81].

Зовнішні ІР формуються зовнішнім інформаційним середовищем і відображають відношення між державою та економічними і політичними суб'єктами, які діють за її межами.

Внутрішні ІР формуються внутрішнім інформаційним середовищем, тобто сукупністю структурних підрозділів держави і працюючих спеціалістів, технічними, соціальними, економічними та іншими відносинами між ними. Внутрішні ІР визначаються внутрішніми бізнес-процесами [82]. При використанні державних ІР, до них пред'являються певні вимоги, в тому числі отримані ІР у визначені терміни, повнота і не спотвореність як вхідних, так і отриманих ІР.

Ефективність бізнес-процесів визначається якістю інформаційних процесів, які реалізуються ІП. Тут важливі натсупні аспекти:

- Вирішальне значення має реальна доступність ІР, яка на практиці обмежена;
- Економічна корисність ІР визначається фактором часу і якістю. Неактуальна або неповна інформація може не тільки виявитися повністю обезціненою, але і призвести до значних втрат вартості вироблених на її основі робіт.

Інформаційні процеси спрямовані на доцільне використання ІР і постачання їх всіх елементів ІП. Ефективність функціонування інформаційних процесів визначається наявністю сучасних засобів обчислювальної техніки, розподілених БД, мереж телекомунікацій, можливістю їх модернізації і модифікації, зміни структури, включення нових компонентів і т.д., що дозволяє забезпечити ефективну циркуляцію і переробку ІР. За призначенням

і характером використання виділимо два основних класи інформаційних процесів:

- системні (ті, які забезпечують) інформаційні процеси - представляють собою процедури виконання окремих системних операцій, пов'язаних з поданням, перетворенням, зберіганням, обробкою або передачею даних;

- прикладні інформаційні процеси - завдання індивідів. Основна мета прикладних інформаційних процесів - отримувати за допомогою переробки первинних ІР інформацію, на основі якої виробляються управлінські рішення.

Будемо вважати, що в ІП циркулюють інформаційні ресурси чотирьох типів:

- $ІР_1$ – початкові дані, що отримані на зберігання і обробку від ДІ (включаючи споживачів і взаємодіючих ІП);
- $ІР_2$ – похідні дані, тобто дані, які отримані в ІП в процесі переробки початкових та похідних даних;
- $ІР_3$ – програми, що використовуються для обробки даних і забезпечення функціонування ІП;
- $ІР_4$ – нормативно-довідкові і службові дані.

Достовірність інформації (ступінь довіри до даних), яка міститься в інформаційних ресурсах $ІР_1$, $ІР_2$, $ІР_3$, $ІР_4$ багато в чому визначається якістю джерела [79]. Отже, необхідно говорити про достовірність інформації як достовірність ДІ (точніше, про ступінь довіри споживача-індивіда до конкретного джерела), який спотворює (неусвідомлено або свідомо) дані, які ним формуються, створюючи інформацію, яка в них міститься недостовірною.

Достовірність ДІ – апостеріорна оцінка, яка отримана в результаті спостереження за його «інформаційною активністю» джерела. Джерелу можна довіряти або ні – тобто суб’єкт може надавати системі дезінформацію, і може бути достойним довіри або недовіри.

Достовірність інформації, яка міститься в $ІР_2$, $ІР_3$, $ІР_4$ в основному визначається якістю і стійкістю процесів (функцій) зберігання, переробки і

представлення даних, які відбуваються в рамках технічної підсистеми ІП при виконані задач індивідів [83, 84]. Така функціональна стійкість системи досягається надійністю технічних і програмних засобів, живучістю структурної побудови системи, кваліфікацією та навиками в роботі персоналу, забезпеченням безпеки ІР [85, 86]. В даному випадку слід пов'язати поняття достовірності інформації с категоріями цілісності та доступності ІР. Цілісність ІР забезпечується, якщо ІР нелегітимно не змінюється, доступність – якщо легітимний процес отримує ІР за прийнятий час. Все це повинно бути забезпечено при функціонуванні ІП в умовах випадкових чи навмисних інформаційних впливів [87].

Отже, кожна ланка проходження (обробки) інформації накладає на неї свій (інформаційний) фільтр, що вносить свої «ослаблення і запізнювання», тобто спотворення. Природа таких спотворень найчастіше випадкова. У підсумку «достовірність інформації», яку ми оцінюємо, є завжди апріорна оцінка ймовірності того, що повідомлення для користувача при вирішенні певного завдання буде містити неспотворені дані.

Урахування факторів інформаційного протиборства на достовірність інформації. Відповідно до загальновизнаної класифікації загроз [88, 89] була складена карта загроз надійності ІР, як показано на рисунку 2.6, та розробив їх розширений перелік. Виявлено такі загрози автентичності:

Саботаж або навмисне загроза навмисне порушення потоку інформації, ухилення або нечесність. Мішенню загроз є персонал (внутрішні порушники-внутрішній персонал), особи (зовнішні порушники). Ця загроза може скористатися організаційною нестабільністю ІП, невдоволенням працівників, наприклад, попитом на робочу силу. Особи легко експлуатуються через їх психофізіологічні особливості. Засобами загрози можуть бути:

- вандалізм - виведення з ладу всіх або окремих елементів ІП (пристроїв, носіїв, персоналу);

- дезорганізація функціонування системи – неправомірне відключення обладнання, зміна режимів роботи технічних засобів (ТЗ) чи програмного забезпечення (ПЗ);
- навмисне зловживання ресурсами (в тому числі мережні);
- зловживання правами;
- впровадження зловмисного ПЗ;
- нелегітимна імперсонація – «маскарад», в тому числі незаконне підключення до ліній зв’язку;
- розголошення, передача чи втрата атрибутів розмежування доступу (паролі, ключі шифрування, пропусків тощо);
- заміна, вставка, видалення чи зміна даних в інформаційному потоці в каналі зв’язку;
- розкриття використовуваних алгоритмів шифрування;
- недобросовісне виконання обов’язків персоналом;

ведення агентурної роботи.

- Несанкціонований доступ до НСД (ІР) є першопричиною несанкціонованих змін, заміни або знищення ІР. Це може знищити цілісність та доступність ІР. Предметом цієї загрози є, як правило, зовнішній зловмисник. Ця загроза може використовувати вразливості ІП: недоліки ІП та його компонентів (наприклад, вразливості програмного забезпечення). В якості засобів загрози може бути:
- нелегітимна імперсонація, розголошення, передача чи втрата атрибутів розмежування доступу;
- впровадження зловмисного ПЗ;
- видалення чи зміна даних в інформаційному потоці в каналі зв’язку;
- розкриття використовуваних алгоритмів шифрування.

Загрози достовірності ІР

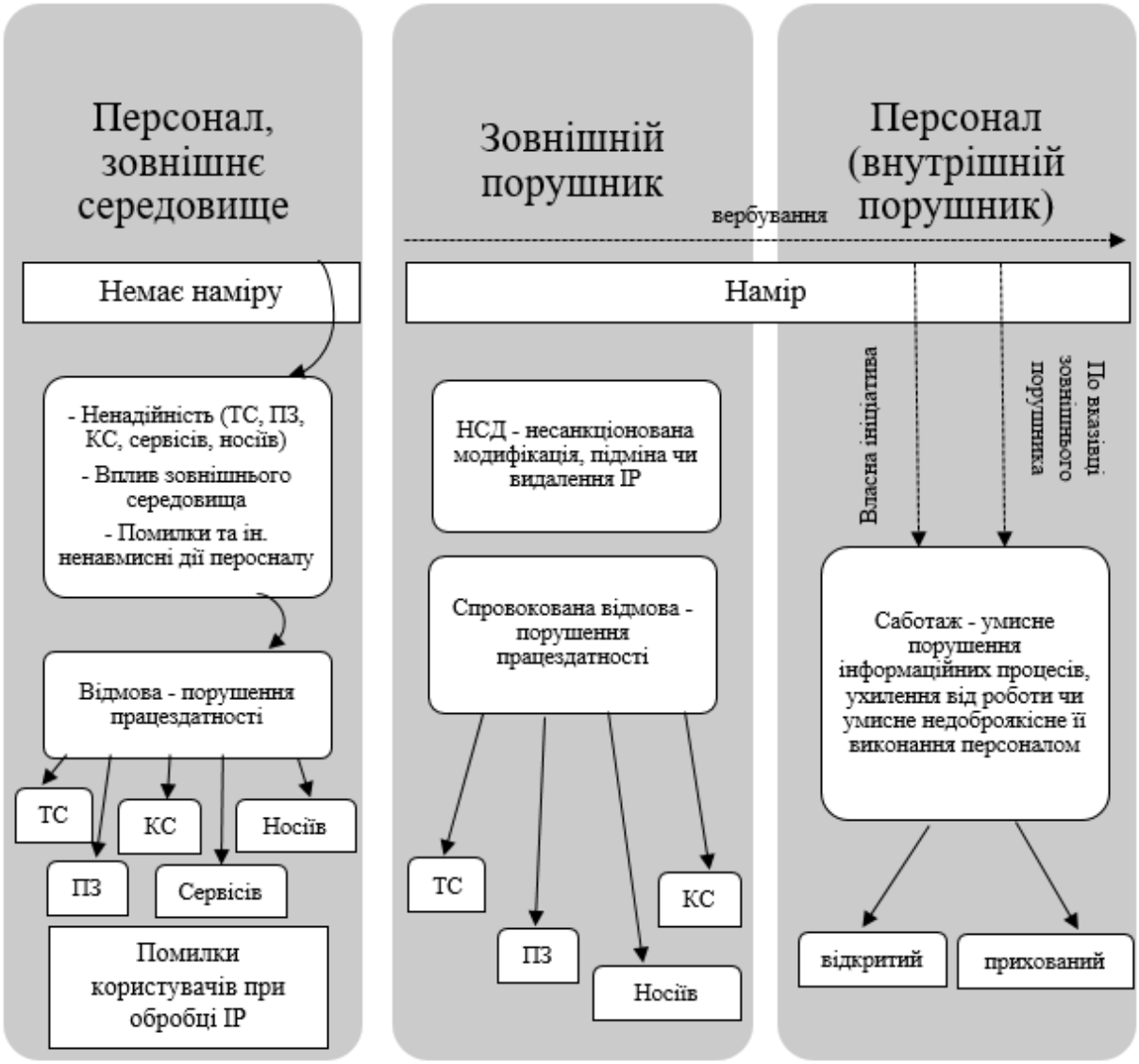

Рис. 2.6. Карта загроз достовірності ІР

- Спровокована відмова – порушення працездатності елементів ІП: ТС, ПЗ. Це може знищити доступність ІР. Ціль цієї загрози - зовнішні порушники. Ця загроза може скористатися вразливістю ІП - недоліками ІП та його елементів. В якості загроз можуть використовуватися:
  - вандалізм;
  - дезорганізація функціонування системи;

- нелегітимна імперсонація, розголошення, передача чи втрата атрибутів розмежування доступу;
- навмисне зловживання ресурсів;
- впровадження зловмисного пз.

1. Відмова обладнання, програмного забезпечення, послуг - це випадкова загроза, що призводить до порушення доступності ІР. Об'єктами, яким загрожує загроза, є: зовнішнє середовище, працівники, виробники скінченних елементів, організації, що надають послуги, та їх працівники. Ця загроза може скористатися слабкими сторонами індивідуальних підприємців: підприємницьке середовище, низька кваліфікація працівників, відсутність досвіду, низька надійність транспортних засобів, програмного забезпечення та засобів масової інформації, структурні дефекти індивідуальних підприємців, дефекти в організаційній підтримці та організаційна невдача. В якості засобів здійснення загрози можуть виступати:

- ненавмисне відключення обладнання чи зміна режимів роботи пристроїв і програм персоналом;
- зловживання ресурсами ІП;
- ненавмисне використання несанкціонованих програм і обробка даних;
- помилки персоналу (при встановленні, налаштуванні обладнання і програм тощо).

2. Особиста помилка в обробці прав інтелектуальної власності - це випадкова загроза, яка може призвести до порушення цілісності та доступності прав інтелектуальної власності. Суб’єкти загрози – індивіди. Ця загроза може використати слабкі сторони індивідуальних підприємців, такі як низька індивідуальна кваліфікація.

Об'єкти, теми або явища, які негативно впливають на надійність ІР через власне існування, збій або цілеспрямований вплив, будуть називатися джерелом загроз достовірності (ДЗД).

Визначення способів забезпечення достовірності інформації. Для забезпечення необхідного рівня достовірності ІР потребується:

- механізми практичної реалізації гарантованого забезпечення необхідного рівня достовірності;
- засоби раціональної реалізації необхідних дій по ЗДІ;
- способи оптимальної організації і проведення всіх дій по ЗДІ в процесі функціонування ІП.

Для побудови концепції, яка задовольняє всім вимогам, пропонується система концептуального рішення (аналогічна концепції інформаційної безпеки) [89]):

- формування повної множини функцій забезпечення достовірності ІР,
- формування повної множини засобів і способів реалізації.

Перерахуємо види способи реалізації:

1) Запобігання виникнення загроз (F_1). Загрози достовірності інформації (ЗагДІ) може виникнути випадково чи навмисно, і її джерелом, як правило, є людина. Тут слід зменшити кількість джерел загроз. Тут слід понижувати кількість джерел загроз. З цієї причини співробітникам служби безпеки слід співпрацювати з інформаторами, щоб контролювати та об'єктивно оцінювати конкурентів та персонал всередині та поза злочинною групою. У цьому запобіганні загрозам на основі поглибленого аналізу місць злочинів та діяльності конкурентів та зловмисних факторів життєво важливу роль відіграє інформаційно-аналітична діяльність відділу безпеки.

2) Стримування загроз (F_2). Основна мета - сприяти побудові архітектури скінченних елементів, впровадженню інформаційного потоку (включаючи програмне та апаратне забезпечення) та впровадженню організаційної структури, щоб мінімізувати можливість лазівок у скінченних елементах, тобто мета попереджувальний страйк.

3) Виявлення загроз, що появилися (F_3). Передбачається, що перед визначенням заходів, що становлять загрозу для прямих іноземних інвестицій, такі заходи слід визначити (отже, використовувати їх) для виявлення загрози прямих іноземних інвестицій. Іншими словами, це функція постійного моніторингу характеристик, що ідентифікують конкретні загрози.

4) Попередження впливу на ІР проявлених загроз (F_4) – заходи, котрі здійснюються в рамках даної функції, яка переслідує мету не допустити небажаного впливу ЗагДІ на ІР, якщо вони реально проявились, тобто дана функція є природнім продовженням попередньої. Це передбачає використання засобів, які «усувають або ослабляють вплив загрози».

5) Виявлення впливу (не виявлених) загроз (F_5) – функція переслідування ІР з метою своєчасного виявлення фактів впливу на них не виявлених (невідомих) ЗагДІ. Отже, за своєчасних засобів реальна можливість локалізації впливу інформації все ще може зберігатися.

6) Усунення (локалізація, обмеження) виявленого впливу загроз (F_6). Як логічне продовження попередньої, ця функція передбачена для запобігання розповсюдженню впливу ("ненадійного") на інші (компоненти) ІР (перевищення максимально допустимого розміру).

7) Ліквідація наслідків реалізованої атаки (F_7) – проведення таких заходів відносно локалізованого впливу ЗагДІ на інформацію, в результаті яких подальша обробка інформації може здійснюватися без врахування впливу, що мав місце бути. Іншими словами, стан інформаційних ресурсів, що стався до впливу ЗагДІ, можна відновити.

Заходи щодо забезпечення надійності ІР шляхом реагування на внутрішні та зовнішні загрози, зменшення впливу ЗагДІ на ІР та сприяння відновленню ІР у процесі реалізації загроз, шляхи та методи реалізації функції забезпечення надійності ІР.

Засоби ЗДІ - це заходи, процедури, механізми та обладнання, які можуть вживати заходів для забезпечення достовірності ІР з різним ступенем ефективності.

В таблиці 2.1. приведено відповідність заходів і способів забезпечення достовірності ІР функціям ЗДІ. Зверніть увагу, що кожна функція забезпечується підмножиною цілого набору заходів та методів.

Таблиця 2.1.

Зв'язок функцій з заходів та способів забезпечення достовірності інформаційних ресурсів

Заходи і засоби ЗДІ	1	2	3	4	5	6	7
Організаційне забезпечення	+	+		+		+	+
Фізичний захист	+	+		+			
Забезпечення цілісності даних			+	+	+		+
Контроль доступу				+			
Ідентифікація та автентифікація				+			
Аудит			+		+		
Контроль носіїв даних		+		+			
Забезпечення надійності інфраструктури	+	+					
Мережне адміністрування		+		+		+	+
Захист від шкідливого ПЗ			+	+		+	+
Виявлення вторгнень			+				
Валідація даних				+	+		

Обгрунтування показників оцінки достовірності інформації. Опис достовірності інформаційного ресурсу здійснюється на основі:

- властивостей інформації, які комплексно визначають категорію «достовірність»;
- множини цілей управління достовірністю, яка визначається прикладними задачами ІП, на базі яких формуються основні критерії забезпечення властивостей;

- множини показників (якісно-кількісних уявлень виміряних характеристик достовірності ІР), порівнянних з критеріями та, що дозволяють віднести оцінювану достовірність ІР до того класу, який визначається виходячи з цілей.

Властивості інформації, які пропонуються для оцінки її достовірності:

- автентичність – відповідність інформації про об'єкт чи появі його дійсному стану;
- повнота – відображення всіх вагомих в рамках задачі характеристик об'єкта;
- актуальність (своєчасність) – відображення характеристик об'єкта або появи з затримкою, допустимою в задачі, що вирішується;
- цілісність – незмінність в процесах зберігання, передачі, обробки і представлення даних в ІП.

Для оцінки достовірності використовуються наступні критерії достовірності:

1) довіра до джерела інформації:

- впевненість в тому, що інформація поступила саме з даного джерела інформації (ДІ);
- впевненість в тому, що дане ДІ володіє повнотою даних для надання конкретної інформації;
- впевненість в тому, що дане ДІ надало всі необхідні (запрошені) дані;
- впевненість в тому, що при передачі в ІП даних від ДІ не допущено спотворення інформації (тобто були присутні певні помилки чи не були внесені дані з брехливою інформацією);

2) Довіра до системи обробки даних в інформаційному просторі:

- впевненість в тому, що дана інформація не спотворена на будь-якому періоді технологічного процесу обробки даних в направлені від ДІ до індивіда;

- впевненість в тому, що запрошені задачею індивіда дані будуть актуальні і доставлені до задачі вчасно;
- довіра до результату.

Порушення відповідних показників свідчать про те, що має місце порушення надійності, тобто ненадійний ІР - це справжній, неповний, непов’язаний або неповний ІР. Якщо ІС структурований, це означає, що певні компоненти ІР є надійними, що призводить до збереження таких понять, як "рівень надійності ІР".

Усі показники надійності динамічні, але лише за показниками кореляції можна встановити функціональну залежність від часу та багатьох характеристик ІП, оскільки це визначається загально визначеним процесом видалення інформації. Стабільність часу індексу цілісності обмежена тимчасовою стабільністю індексу цілісності та вимогами об'єктної інформаційної моделі з наступних. Індекс цілісності визначається випадковим процесом і може бути передбачений з певною ймовірністю. Індекс автентичності залишається незмінним з точки зору цілісності індексу кореляції та постійності індексу цілісності.

Таким чином, концептуальна модель достовірності інформації включає: інформаційні ресурси, джерела інформації, фактори інформаційного протиборства, джерела факторів інформаційного протиборства (загроз достовірності), цілі зловмисників, функції, методи та засоби забезпечення достовірності, показники достовірності. Достовірність інформації (ступінь довіри до даних), яка міститься в інформаційних ресурсах багато в чому визначається якістю джерел та можливістю індивідів впливати на інформаційні процеси. При цьому поняття достовірності інформації часто пов’язується з категоріями цілісності та доступності інформаційних ресурсів. Все це повинно бути забезпечено при функціонуванні інформаційного простору в умовах випадкових чи навмисних інформаційних впливів.

Основні загрози достовірності інформаційним ресурсам реалізуються через фактори інформаційного протиборства: навмисне порушення інформаційного процесу, несанкціонований доступ, порушення працездатності елементів, помилки суб'єктів інформаційного обміну. Основні способи протидії загрозам – запобігання, виявлення та стримування загроз; упередження, виявлення, усунення та ліквідація наслідків інформаційного впливу. Для формування критеріального апарату у якості найбільш доцільних можуть бути обрані дві групи показників достовірності інформації, які відображають довіру до: 1) джерела інформації; 2) системи обробки даних в інформаційному просторі. Всі показники достовірності є динамічними, але при цьому тільки для показника актуальності можна встановити функціональну залежність від часу і ряду характеристик інформаційного простору, так як він визначається в цілому детермінованими процесами усунення інформації.

2.4. Розробка моделі управління достовірністю інформації в умовах інформаційного протиборства

Формування підходу до управління достовірністю інформації. Розглянемо модель функціонування ІП з точки зору виникнення і реалізації ФІП (загроз ДІ), а також протидії їм заходів забезпечення достовірності (рис. 2.7).

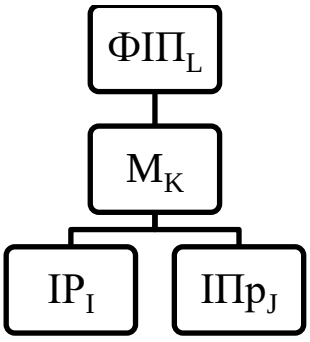

Рис. 2.7. Модель функціонування інформаційного простору в умовах інформаційних впливів

Допустимо, що в ІП визначені і класифіковані наявні «вразливості», такі як системні уразливості (СУ), складений повний перелік можливих ФІП і заходів забезпечення достовірності. Позначимо через *n* загальне число ФІП, *s* – число СУ, *x* – число заходів забезпечення достовірності ІР та інформаційних процесів.

I-й ФІП можна охарактеризувати відносною частотою виникнення $p_I^{ФІП}$. Сукупність елементів системи забезпечення достовірності інформації (СЗДІ) можна охарактеризувати показниками якості захисних заходів передачі, збереження і обробки *i*-го ІР в умовах впливу *I*-ого ФІП: $x_{iI}^{П}$, $x_{iI}^{Х}$, $x_{iI}^{О}$. Ці заходи знижують ймовірність порушення достовірності *i*-го ІР *I*-м ФІП $p_{iI}^{НД}$ шляхом забезпечення автентичності (скорочення числа помилок в процесі обробки) і цілісності (недопущення спотворень в процесі зберігання і передачі).

Оцінюючи повноту інформації, потрібно враховувати характеристики джерела інформації (ДІ). Області знань ДІ відповідає повний тезаурус ключових понять *T*. Область знань може бути розділена на ряд предметних областей з окремими тезаурусами $T_к$. здатність джерела до надання необхідної інформації з галузі знань визначається відповідністю предметних областей.

Зробивши запит на дані, надані ДІ (якщо дані будуть надані на запит) або область, що цікавить одержувача інформації (якщо збір інформації здійснюється без запиту, джерело інформації доступне) покриває *A*-предметні

області з тезаурусами $\mathrm{T_a}, \mathrm{a} \in \mathrm{A}$. нехай інформація від ДІ в даному повідомленні покриває *B*-предметних областей з тезаурусами $\mathrm{T}_b, b \in B$. Тоді можливі наступні стани інформованості ДІ по запиту:

- надлишкова інформованість – множина предметних областей ДІ включає множину предметних областей запиту - $A \subset B$. Тоді ступінь відповідності предметних областей *S=1*;
- повна інформованість – це множина предметних областей джерела та множина предметних областей запиту співпадають - $A = B$. Ступінь відповідності предметних областей *S=1*;
- неповна інформованість – це множина предметних областей ДІ і множина предметних областей запиту частково співпадають, але не рівні - $A \cap B \neq 0, A \neq B$. Ступінь відповідності предметних областей $S = \sum_{\forall a \in A} T_A \,/\, \sum_{\forall b \in B} T_b$;
- неінформованість ДІ – це множина предметних областей ДІ і множина предметних областей запиту не співпадають - $A \cap B = 0$. Ступінь відповідності предметних областей *S=0.*

Показники достовірності *i*-го ІР, отриманого з *j*-ого ДІ в умовах впливу на ІР *n* дестабілізуючих факторів рівний

$$D_{ij} = S_j \cdot \left(1 - \sum_{I=1}^{n} p_I^{\text{ФІП}} \cdot p_{iI}^{\text{НД}}\right) = S_j \cdot \left(1 - \sum_{I=1}^{n} p_I^{\text{ФІП}} \cdot \left(1 - x_{iI}^{\text{П}} \cdot x_{iI}^{X} \cdot x_{iI}^{O}\right)\right), \qquad (2.33)$$

де $p_I^{\text{ФІП}}$ – відносна частота виникнення l-ого ФІП,

$p_{iI}^{\text{НД}}$ – можливість порушення достовірності (знищення, модифікація) і-го ІР І-м ФІП, яка залежить від якості елементів СЗІД

$$p_{iI}^{\text{НД}} = 1 - \left(1 - \prod_{q_1}\left(1 - \delta_{iIq_1}^{\text{П}} \cdot x_{iIq_1}^{\text{П}}\right)\right) \cdot \left(1 - \prod_{q_2}\left(1 - \delta_{iIq_2}^{X} \cdot x_{iIq_2}^{X}\right)\right) \cdot \left(1 - \prod_{q_3}\left(1 - \delta_{iIq_3}^{O} \cdot x_{iIq_3}^{O}\right)\right), \quad (2.34)$$

де $x_{iIq_1}^{\text{П}}$, $x_{iIq_2}^{X}$, $x_{iIq_3}^{O}$ – показники якості q-ого засобу захисту відповідно процесу передачі, зберігання чи обробки *i*-го ІР в умовах впливу *I*-го ФІП;

$0 \le \delta_{iIq} \le 1$ - межа достатності q-го засоби захисту за умови, що воно є єдиним засобом по протидії l-му ФІП, який здатний порушити достовірність і-го ІР.

З формальної точки зору забезпечення надійності інформації в ІП розглядається як дискретна задача управління багатоступеневим процесом із заданим (кінцевим) станом достовірності інформаційних ресурсів $P_{\hat{e}}$, відомим початковим станом P_0 і набором допустимих дій D таких, що дія $d_i \in D$, реалізована на *i*-му кроці, переводить достовірність інформаційних ресурсів з стану P_i в стан P_j з більш високими показниками (достовірності). Задача управління полягає у виборі оптимальної послідовності дій $D^* = \langle d_0^*, d_1^*, \dots \rangle$ і, відповідно, станів $P^* = \langle p_0^*, p_1^*, \dots \rangle$, таких, що в результаті досягається бажане (чи максимально можливо - екстремальне) значення достовірності.

Формальна модель управління достовірністю інформації. Візьмемо як приклад ІР, розглянемо процес управління надійністю інформації, а потім запропонуємо мультимодель на цій основі. Метою управління є надійність ІР. Стан достовірності буде описуватись ідентифікатором *P*, який являє собою вектор окремих показників достовірності $P = \{pd_1, \dots\}$.

Об’єкт управління може піддаватися впливам двох видів:

а) неуправляючі. Це вплив зовнішнього середовища *U(t)*. Зовнішнім середовищем (середовищем) ІР є «ІП» та його безліч структурних елементів та інформаційних процесів. Елементи та інформаційні процеси, ініційовані

відповідним програмним забезпеченням, можуть бути ненадійними та вразливими до інформаційних атак зловмисників, тому сама ОТС має певний ступінь функціональної стабільності та структурної живучості. Цей ефект завжди призводить до "погіршення" показників надійності.

б) цілеспрямовані (управляючі) взаємодії $X \in D$, що функціонально складаються з впливів $X^{(1)}$, які забезпечують (чи підвищують) ті чи інші показники достовірності, і впливів $X^{(2)}$, які контролюють поточні значення даних показників. Нехай ці впливи генеруються спеціальною системою забезпечення надійності інформації (СЗДІ), яка є результатом обробки результатів вимірювань об'єкта та стану довкілля, обраного алгоритму (стратегії), виділених ресурсів та рішення. Завдання досягнення мети.

Процес управління достовірністю ІР представлений на рис. 2.8.

На схемі модель ІР представлена автоматом: перетворювачами $F^{(1)}$ та $F^{(2)}$, а також модулем, який дає змогу зберігати ідентифікатор достовірності (ІД), поточні значення показників, пам'ять стану (ПС) достовірності ІР. Перетворювач $F^{(1)}$ реалізує функцію переходів до нового стану ІД $P(t+1)$ в залежності від його поточного стану $P(t)$, стану середовища $U(t)$ і впливу $X^{(1)}(t)$:

$$P(t+1) = F^{(1)}\{P(t), U(t), X^{(1)}(t)\} \qquad (2.35)$$

Оцінку ідентифікатора достовірності $P^*(t)$ для чергового кроку вироблення керуючих впливів отримують за результатами «вимірювання» показників $P(t)$. Дана процедура ініціюється контролюючим впливом $X^{(2)}(t)$:

$$P^*(t) = F^{(2)}\{P(t), X^{(2)}(t)\} \qquad (2.36)$$

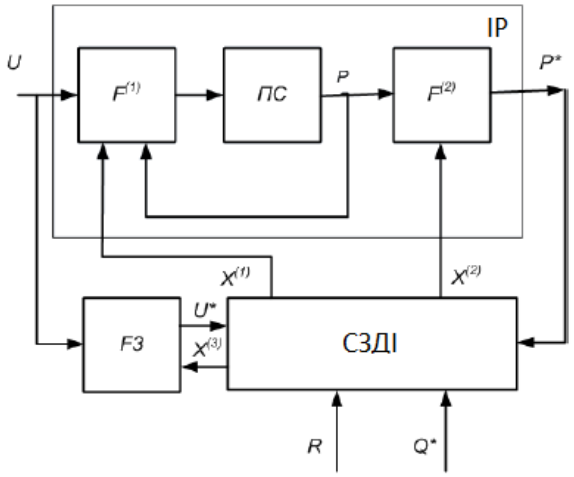

Рис. 2.8. Процес управління достовірністю ІР

Вид функції виходів (перетворювач $F^{(2)}$) багато в чому визначається способом і методикою контролю (вимірювання) показників ІД.

Входи автомата – управління $X \in D$ ($X^{(1)}$ і $X^{(2)}$), що виробляються управляючим пристроєм (СЗДІ) відповідно алгоритму управління ϕ, обраному з множини Φ відомих алгоритмів $\phi \in \Phi$ (стратегії досягнення конкретної мети Q^*), виділених ресурсів R, отриманої інформації про стан середовища U^* і оцінки стану об'єкта P^*:

$$X = \phi(Q^*, P^*, U^*, R) \tag{2.37}$$

Інформацію про стан зовнішнього середовища $U(t)$ для чергового кроку вироблення управляючих впливів доставляють «датчики», здійснюючі функціональне перетворення $F^{(3)}$, у вигляді вимірюваних значень $U^*(t)$. Контроль здійснюється у відповідності з взаємодією з $X^{(3)}$:

$$U^*(t) = F^3\{U(t), X^{(3)}\} \tag{2.38}$$

Стратегія (алгоритм) управління ϕ, в загальному плані, повинна мінімізувати число кроків управління (час досягнення цілі Q^*) для досягнення P_k.

Модель управління достовірністю множини інформаційних ресурсів представлена на рис. 2.9.

Забезпечення достовірності інформації в ІП здійснюється одночасно по N інформаційним ресурсам (IP_1, …, IP_N), представлених в моделі кортежу типу $\langle F_i^{(1)}, ПС_i, F_i^{(2)} \rangle, i = 1, \dots, N$. Це множинний об'єкт управління.

«Функціонування» моделі об'єкта описується системою:

$$\begin{cases} P_1(t+1) = F_1^{(1)}\left\{P_1(t), U_1(t), \dots, U_M(t), X_1^{(1)}\right\} \\ \dots \\ P_N(t+1) = F_N^{(1)}\left\{P_N(t), U_1(t), \dots, U_M(t), X_N^{(1)}\right\} \end{cases} \quad (2.37)$$

де $P_1(t)$, …, $P_N(t)$ – поточний «стан» ІР – значення показників індикаторів достовірності;

$U_1(t), \dots, U_M(t)$ – множина поточних значень параметрів факторів, дестабілізуючих стійке функціонування ІП і які призводять до зниження показників достовірності. Будемо вважати, що дані значення однакові для всіх ІР;

$X_1^{(1)}(t), \dots, X_N^{(1)}(t)$ – управляючі впливи.

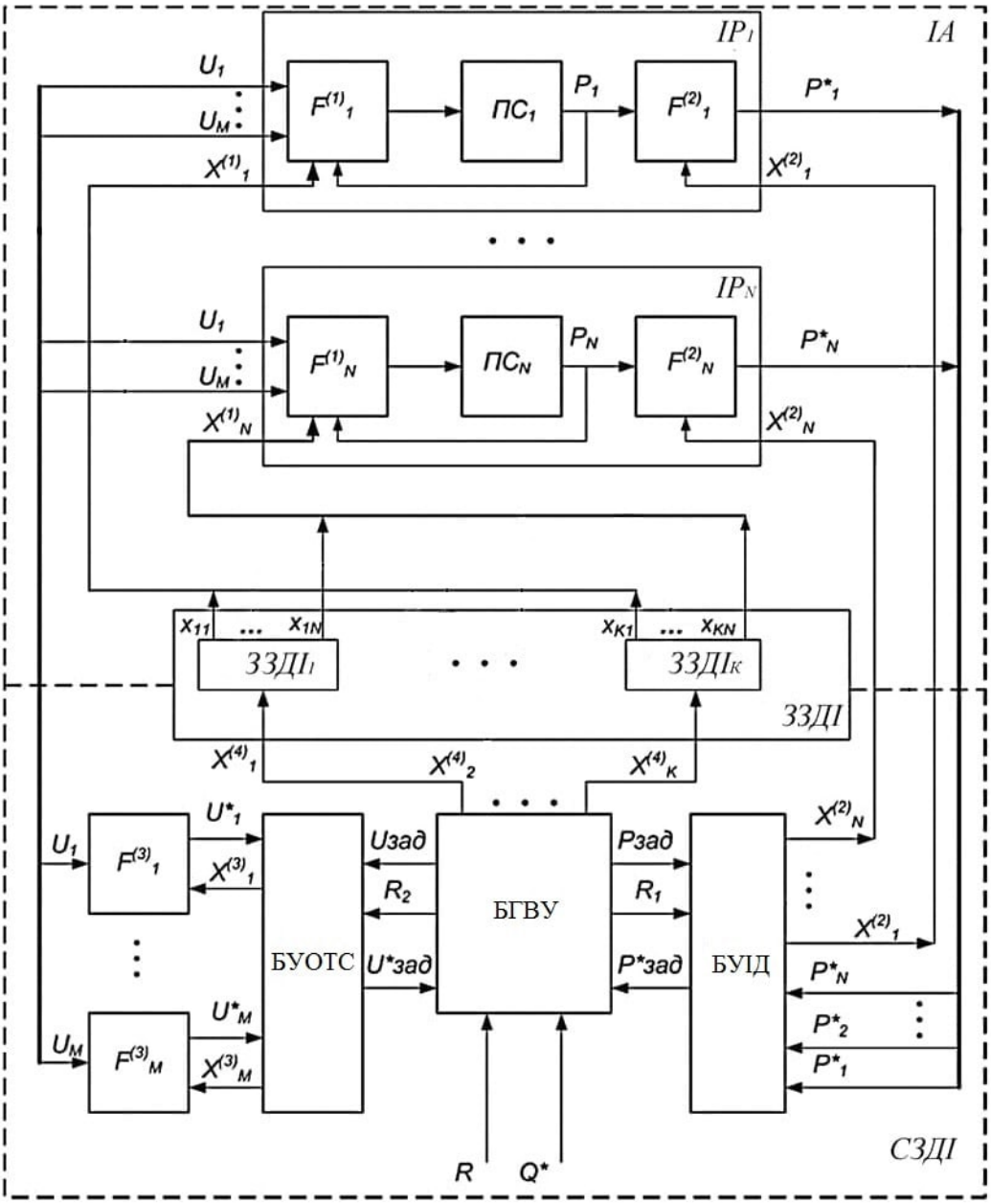

Рис. 2.9. Схема управління достовірністю множини ІР

Множина $\{x_{11}(t), \dots, x_{1K}(t), \dots, x_{N1}(t), \dots, x_{NK}(t)\}$ – множина поточних значень характеристик засобів забезпечення ДІ. Підмножини виду $X_i^{(1)}(t) = \{x_{i1}(t), \dots, x_{iK}(t)\}, i = 1, \dots, N$, як «сукупна» участь засобів забезпечення ДІ, визначають «рівень протидії» дестабілізації ІП по відношенню до IP_i.

Засобом забезпечення ДІ насправді є механізм виконання системи управління, який може поліпшити (або, принаймні, не зменшити) надійність.

Система підтвердження інформації включає блок генерування впливу управління (БГВУ), блок управління ідентифікатором достовірності (БУІД) та блок контролю ОТС (БУОТС).

Основним призначенням БГВУ є формування програми підвищення достовірності (ППД) – оптимальної послідовності дій $D^* = \langle d_0^*, d_1^*, \dots \rangle$ (і відповідно, станів $P^* = \langle p_0^*, p_1^*, \dots \rangle$) таких, що в результаті досягається бажане (чи максимально можливе) значення достовірності. Дії d_j^*, крім контрольних, забезпечують виробку сигналів управління $\left(X_1^{(4)}, \dots, X_K^{(4)}\right)$ засобами забезпечення достовірності інформації, включаючи вибір (ініціювання) певного засобу і завдання режимів його функціонування.

Процес формування ППД D^* виробляється на основі:

- поточного стану об’єкту (вимірювання значення показників ідентифікаторів достовірності $\{P_1^*(t), \dots, P_N^*(t)\}$) і зовнішнього середовища (значення, що вимірюються $\{U_1^*(t), \dots, U_N^*(t)\}$);
- наявних на поточний момент часу засобів забезпечення ДІ, "не задіяних» в інших ППД;
- набору типових процедур управління - функцій і заходів забезпечення достовірності, які кошти забезпечення ДІ потенційно здатні реалізувати;
- виділеного ресурсу R (наприклад, часу) і мети Q^*. Під метою в загальному розумінні розуміється задача на забезпечення (підвищення) визначених показників достовірності конкретних ІР.

Складність процесу формування ППД полягає в тому, що для всіх ІР спосіб надання ДІ однаковий, а вимоги до ймовірності для конкретних цілей також різні. Q^* поширюються на кожен ІР окремо.

БУІД вимірює (оцінює) поточні важливі показники ідентифікаторів надійності.В залежності від виділеного БГВУ ресурсу R_1 на контроль запитуваної підмножини ідентифікаторів достовірності $P_{зад}$ блок виробляє

множину $\left\{X_1^{(2)}, \dots, X_N^{(2)}\right\}$ методик вимірювання (оцінювання) параметрів. В результаті перетворень $F_i^{(2)}, i = 1, \dots, N$ отримуємо оцінки $P_1^*(t), \dots, P_N^*(t)$.

Вимірювання (оцінка) поточного значення характеристик ІП (живучість, надійність, індекс інформаційної активності зловмисника тощо) проводиться БУОТС. В залежності від виділеного БГВУ ресурсу R_2 на контроль запитуваної підмножини поточних характеристик ІП $U_{зад}$ блок виробляє множину $\left\{X_1^{(3)}, \dots, X_N^{(3)}\right\}$ методик вимірювання (оцінювання) характеристик. В результаті датчиків $F_i^{(3)}, i = 1, \dots, M$ отримуємо оцінки $U_1^*(t), \dots, U_M^*(t)$.

При стандартизованому підході до управління надійністю (наприклад, за допомогою строго визначених стандартів для досягнення показників ІД та обмеженого часу) завдання полягає у пошуку системи із найменшими витратами, тобто потрібно вирішити наступні проблеми:

$$\begin{cases} \sum_{i=1}^{N} \sum_{j=1}^{NS} c_{ij}\left(p_{0_{ij}}, t_{\text{зат}_{ij}}\right) \to min, \\ \quad \tilde{p}_{ij}\left(p_{0_{ij}}, t_{ij}\right) > p_{\text{баж}_{ij}}, \\ \quad max_{ij}\left(t_{\text{зат}_{ij}}\right) \le t_{\text{доп}}. \end{cases} \tag{2.38}$$

де c_{ij} - «приведена вартість» підвищення достовірності j-го показника ($j = 1, \dots, NS$) ідентифікатора достовірності i-го ІР ($i = 1, \dots, N$);

$p_{0_{ij}}$ – початковий рівень j-го показника ІД i-го ІР;

$t_{\text{зат}_{ij}}$ – час, необхідний для досягнення $p_{\text{баж}_{ij}}$ – бажаного рівня j-го показника ІД i-го ІР;

$\tilde{p}_{ij}$ – досягнутий (від $p_{0_{ij}}$) за час t_{ij} рівень j-го показника ідентифікатора достовірності i-го ІР;

$t_{\text{доп}}$ – допустимий час, який виділяється на підвищення достовірності ІР;

N – загальна кількість ІР;

NS – кількість показників ІД.

Ближче до фактичного завдання - максимізувати показники ІД при обмежених ресурсах та допустимих витратах $C_{доп}$

$$\begin{cases} \sum_{i=1}^{N}\sum_{j=1}^{NS} \tilde{p}_{ij}\left(p_{0_{ij}}, t_{\text{зат}_{ij}}\right) \to max, \\ \tilde{p}_{ij}\left(p_{0_{ij}}, t_{ij}\right) > p_{\text{баж}_{ij}}, \\ max_{ij}\left(t_{\text{зат}_{ij}}\right) \le t_{\text{доп}}, \\ \sum_{i=1}^{N}\sum_{j=1}^{NS} c_{ij}\left(p_{0_{ij}}, t_{\text{зат}_{ij}}\right) \le C_{\text{доп}}. \end{cases} \quad (2.39)$$

Таким чином, основний підхід до управління достовірністю інформації має базуватися на моделі функціонування інформаційного простору з урахуванням можливості виникнення і реалізації факторів інформаційного протиборства. На основі теоретико-множинного підходу будується система класифікації наявних вразливостей та можливих факторів інформаційного протиборства і, відповідних їм, заходів забезпечення достовірності інформації. З формальної точки зору управління достовірністю інформації в інформаційному просторі розглядається як задача дискретного управління багатокроковим процесом з заданим бажаним (кінцевим) станом достовірності інформаційних ресурсів при відомому початковому стані і наборові допустимих дій. При цьому дія, реалізована на окремому кроці, переводить достовірність інформаційних ресурсів з початкового стану до стану з більш високими показниками достовірності. При нормативному підході до управління достовірністю (наприклад, при строго визначеному критерії досягнення показників достовірності) найбільш доцільним є зведення завдання управління до пошуку рішення з мінімальною вартістю.

Висновки до розділу 2

1. У контексті розгляду активних інформаційних дій актуальним є питання розроблення математичних моделей, які описують процеси інформаційної війни та інформаційного протиборства. Базова модель інформаційного впливу базується на динаміці зміни числа прихильників інформаційного повідомлення – тобто тих, хто сприймає інформацію через визначений канал комунікації. На відміну від моделі інформаційного впливу, модель інформаційного протиборства передбачає наявність двох конфліктуючих інформаційних потоків, які розповсюджуються серед суспільства. Побудова моделей у вигляді диференційних рівнянь дає можливість досліджувати динаміку розповсюдження інформації. При цьому визначення “переможця” чи “переможеного”, залежить від того, яка сторона змогла розповсюдити свою інформацію серед більшого, ніж суперник, числа членів спільності до моменту повного охоплення соціуму обома видами інформації.

2. Запропонована базова модель інформаційного впливу може бути розширена за рахунок введення складових, які відображають процеси: забування інформації індивідами, неповного охоплення соціуму засобами масової інформації, багатократного засвоєння та забування інформації. Крім того, можливе також розширення моделей за рахунок включення передбачення про поділ соціуму на дві групи населення, кожна з яких характеризується своїми значеннями додаткових параметрів (інтенсивність розповсюдження інформації через ЗМІ та під час особистої комунікації). Подальшим удосконаленням моделі є урахування процесів засвоєння інформації, які передбачають багатократне проведення інформаційних кампаній. Отже, результуюча узагальнена модель інформаційної протидії включає систему диференційних рівнянь, які описують зміну кількості

прихильників інфомаційних повідомлень, що належать до різних груп у залежності від параметрів груп та частоти появи повідомлень.

3. Концептуальна модель достовірності інформації включає: інформаційні ресурси, джерела інформації, фактори інформаційного протиборства, джерела факторів інформаційного протиборства (загроз достовірності), цілі зловмисників, функції, методи та засоби забезпечення достовірності, показники достовірності. Достовірність інформації (ступінь довіри до даних), яка міститься в інформаційних ресурсах багато в чому визначається якістю джерел та можливістю індивідів впливати на інформаційні процеси. При цьому поняття достовірності інформації часто пов’язується з категоріями цілісності та доступності інформаційних ресурсів. Все це повинно бути забезпечено при функціонуванні інформаційного простору в умовах випадкових чи навмисних інформаційних впливів.

4. Основні загрози достовірності інформаційним ресурсам реалізуються через фактори інформаційного протиборства: навмисне порушення інформаційного процесу, несанкціонований доступ, порушення працездатності елементів, помилки суб’єктів інформаційного обміну. Основні способи протидії загрозам – запобігання, виявлення та стримування загроз; упередження, виявлення, усунення та ліквідація наслідків інформаційного впливу. Для формування критеріального апарату у якості найбільш доцільних можуть бути обрані дві групи показників достовірності інформації, які відображають довіру до: 1) джерела інформації; 2) системи обробки даних в інформаційному просторі. Всі показники достовірності є динамічними, але при цьому тільки для показника актуальності можна встановити функціональну залежність від часу і ряду характеристик інформаційного простору, так як він визначається в цілому детермінованими процесами усунення інформації.

5. Основний підхід до управління достовірністю інформації має базуватися на моделі функціонування інформаційного простору з

урахуванням можливості виникнення і реалізації факторів інформаційного протиборства. На основі теоретико-множинного підходу будується система класифікації наявних вразливостей та можливих факторів інформаційного протиборства і, відповідних їм, заходів забезпечення достовірності інформації. З формальної точки зору, управління достовірністю інформації в інформаційному просторі розглядається як задача дискретного управління багатокроковим процесом з заданим бажаним (кінцевим) станом достовірності інформаційних ресурсів при відомому початковому стані і наборові допустимих дій. При цьому дія, реалізована на окремому кроці, переводить достовірність інформаційних ресурсів з початкового стану до стану з більш високими показниками достовірності. При нормативному підході до управління достовірністю (наприклад, при строго визначеному критерії досягнення показників достовірності) найбільш доцільним є зведення завдання управління до пошуку рішення з мінімальною вартістю.

РОЗДІЛ 3.
РОЗРОБКА МЕТОДИКИ ОЦІНКИ ДОСТОВІРНОСТІ ІНФОРМАЦІЇ В УМОВАХ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА

3.1. Оцінка передумов формування методики оцінки достовірності інформації

Забезпечення необхідного рівня достовірності інформації, що циркулює в ІП, неможливо без оцінки поточного рівня, який визначають безліч різних чинників. Методика оцінки поточного рівня достовірності інформації як ймовірності збереження її незмінності в інформаційному потоці в умовах інформаційних впливів вимагає дослідження наступних критеріїв [91-96]:

- відносні частоти виникнення дестабілізуючих факторів - ФІП (загроз достовірності) $Р_{ФІП}$,
- можливості порушення достовірності інформації $Р_{НД}$.
- ймовірності виявлення спроб порушення достовірності $Р_{В}$.

Відповідно, підвищення рівня достовірності в умовах інформаційних впливів можливо роботою в трьох напрямках [97]:

- зміна структури ІП з метою зменшення кількості вразливостей/структурно-функціональних недоліків (СУ), призводять до виникнення ФІП;
- підвищення якості системи забезпечення достовірності інформації (СЗДІ).

Необхідною умовою досягнення необхідного рівня достовірності інформації (ДІ) є побудова комплексної СЗДІ. ІП підприємств існують в системі товарно-грошових відносин, в основі якої лежить поняття економічної ефективності, і не можуть собі дозволити безконтрольно і безпідставно

витрачати матеріальні ресурси на проведення будь-яких заходів. Внаслідок цього оцінка рівня ДІ і прийняття рішень щодо проведення заходів для його підвищення піднімають супутню завдання оцінки економічного ефекту від їх проведення.

Отже, в загальний метод оцінки достовірності необхідно включити такі додаткові критерії:

- вартість інформаційних ресурсів (ІР) S_{IP},
- вартість засобів обробки інформації S_{OI},
- вартість системи забезпечення достовірності $S_{СЗДІ}$,
- сумарний ризик інформації $R_{IP,}$
- сумарний ризик засобів обробки інформації R_{OI},
- сумарний ризик системи забезпечення достовірності $R_{СЗДІ}$.

Імовірнісні, вартісні критерії та критерії ризиків можна назвати параметрами ІП. Залежать від них загальний коефіцієнт достовірності інформації D_{IP} і економічна ефективність E_f є *показниками якості* СЗДІ.

Можна виділити наступні залежності між параметрами ІП:

$$
\begin{aligned}
P_{ФІП} &= f\,(S_{IP}, S_{OI}),\\
P_{НД} &= f\,(P_{ФІП}, S_{IP}, S_{OI}, S_{СЗДІ}),\\
R_{IP} &= f\,(S_{IP}, S_{СЗДІ}, P_{ФІП}, P_{НД}),\\
R_{OI} &= f\,(S_{OI}, S_{СЗДІ}, P_{ФІП}, P_{НД}),\\
R_{СЗДІ} &= f\,(S_{СЗДІ}, P_{ФІП}, P_{НД}).
\end{aligned}
\qquad (3.1)
$$

Оцінка поточного рівня ДІ не є самоціллю, вона необхідна для оптимізації параметрів ІП з метою підвищення ДІ в ІП в умовах інформаційних впливів. Загальна модель контролю показників ДІ в ІП представлена на рис. 3.1.

Залежності (3.1) носять імовірнісний характер. Математична статистика і теорія ймовірностей використовують експериментальні дані, володіють точністю і достовірністю [98, 99]. В даному випадку поняття точності і достовірності не завжди застосовні, тому що ці ймовірності залежать від «людських знань» [100]. Тому для достовірної кількісні оцінки показників якості СЗДІ необхідно використовувати теорію нечітких множин, яка оперує не поняттям «ймовірність», а поняттям «можливість», що більш адекватно відповідає рішенню важко формалізованих завдань.

Ймовірності виникнення, виявлення та усунення помилок є числовими характеристиками і можуть бути визначені статистичними методами. Але ІП складається з множини різнорідних компонентів, їх склад може вельми істотно відрізнятися. Тобто отримати статистику по достатній кількості однотипних систем майже завжди неможливо. Рішенням тут може бути експертна оцінка. Для показників достовірності та ефективності необхідно отримання кількісного результату, що істотно ускладнюється низкою факторів:

- наявність складної опосередкованої взаємозв'язку цих показників з параметрами ІП;
- необхідність обліку та формалізації ряду параметрів ІП, багато з яких спочатку задані якісними величинами і мають елементи неоднозначності;
- наявність суттєвого взаємозв'язку і взаємозалежності цих параметрів, що мають суперечливий характер;
- складність отримання вихідних даних, необхідних для оцінки, зокрема на ранніх етапах проектування СЗДІ.

Проектування, організація і застосування СЗДІ фактично пов'язані з невідомими подіями в майбутньому і тому завжди містять елементи невизначеності. Крім того, присутні й інші причини неоднозначності, такі як недостатньо повна інформація для прийняття управлінських рішень або соціально-психологічні чинники.

У процесі виконання завдання оптимізації доводиться враховувати наступне [101]:

- переважно нечіткий опис множини вихідних даних, зокрема опис стандартів, які використовуються при побудові СЗДІ і задаються у вигляді вимог;
- сама постановка завдання вибору зазвичай є нечіткою, при цьому перевагу того чи іншого показника визначається експертною інформацією;
- багатокритеріальність завдання.

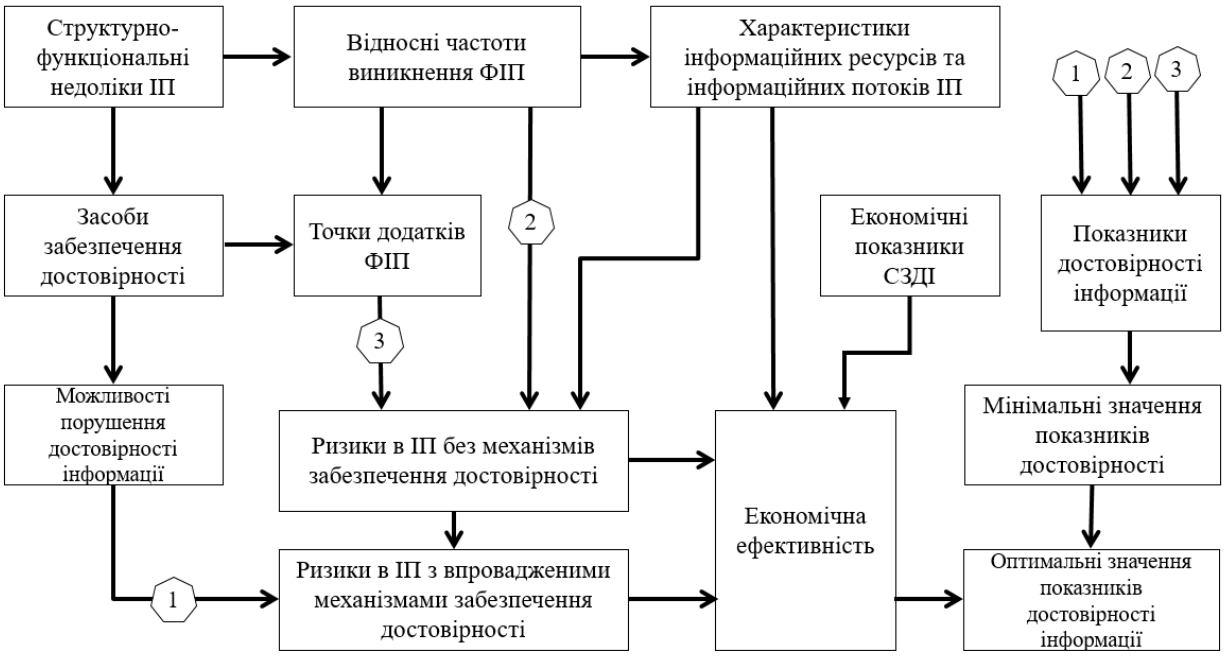

Рис. 3.1. Загальна модель контролю показників достовірності інформації в ІП

З економічної точки зору ефективним буде такий комплекс заходів щодо підвищення достовірності інформації в ІП, при якому виконані наступні умови:

$$\begin{cases} Scзд \le \Delta Rip + \Delta Roi + \Delta Rcзд \\ Scзд \le Sip + Soi \end{cases} \quad (3.2)$$

де $\Delta R_I + \Delta R_{OI} + \Delta R_{CЗI}$ - загальне зниження ризиків в ІП.

Якщо перша умова очевидно: отриманий ефект не повинен бути менше вартості коштів і заходів, тобто витрат, то друге не настільки очевидно. І тим не менше, дійсно велика частина витрат підприємства спрямована на виконання його основної діяльності, а не на реалізацію функцій СЗДІ.

З функціональної точки зору, яка визначена загальним коефіцієнтом достовірності, якість системи визначають умови, показують відповідність деякому мінімального порогу, наприклад, так:

$$D_i \; D_{i,min}, \; \forall \; i = \overline{1,z} \tag{3.3}$$

Умови (3.2) і (3.3), очевидно, суперечливі: підвищення рівня ДІ в ІП на певному етапі можливо тільки при збільшенні інвестицій в СЗДІ. З цього випливає постановка задачі оптимізації:

$$\begin{cases} D_{IP} \; \rightarrow \max \\ D_i \geq D_{i.min}, \forall \; i = \overline{1,z}, \\ S_{СЗД} \leq \; \Delta R_{IP} + \; \Delta R_{OI} + \; \Delta R_{СЗД} \\ S_{СЗД} \leq \; S_{IP} + \; S_{OI} \end{cases} \tag{3.4}$$

Модель контролю показників достовірності інформації в ІП, представлена на рис. 3.1, є спільною, відображає структуру взаємозв'язків параметрів ІП, а також порядок їх оцінки. Характер взаємозв'язків можна описати моделлю, представленої на рис. 3.2.

Область ФІП *T* являє собою список всіх можливих ФІП для даної ОТС, кожен ФІП характеризується відносною частотою виникнення.

Множина СУ *V* являє собою перелік всіх існуючих вразливостей в даній ОТС, основними характеристиками яких є значимість і доступність для зловмисника. В сукупності множини ФІП та СУ і їх взаємозв'язку утворюють перелік способів досягнення мети - інформаційний вплив на ІР організації

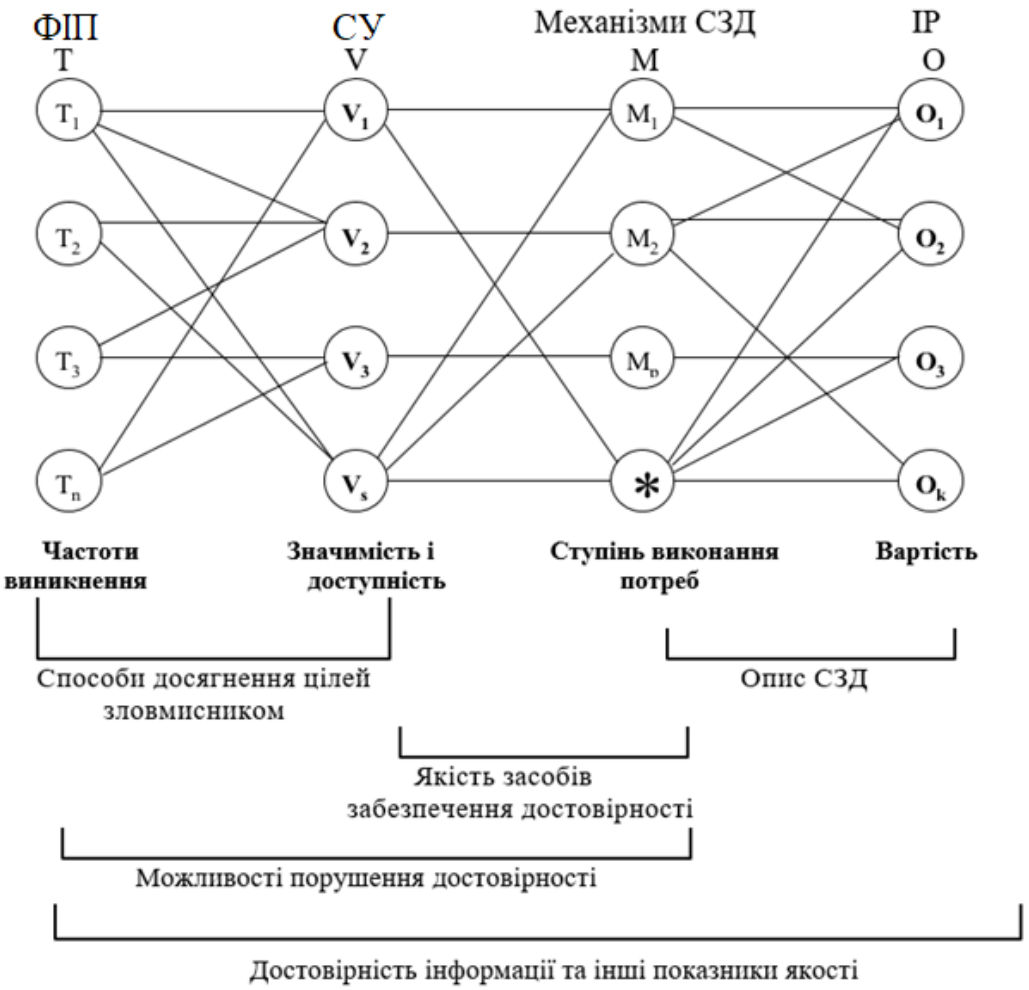

Рис. 3.2. Модель, що описує характер взаємозв'язку параметрів ІП і показників якості СЗДІ

набір засобів забезпечення достовірності. Якість засобів забезпечення достовірності визначається при розгляді множини *V* і множини *M* з їх взаємозв'язками, і характеризується можливостями подолання кожного бар'єру, асоційованого з кожним СУ.Тут штучно доданий елемент **(*)**, що показує, що ряд СУ, може бути взагалі не перекритий будь-яким бар'єром.

Область *O* представляє собою сукупність ІР, характеристики яких: цінність і вартість, яка визначається виходячи з фінансових втрат організації, асоційованих з відновленням ресурсу, або з упущеною вигодою, пов'язаними зі знищенням, тиражуванням, або блокуванням доступу до захищеного ресурсу.

Разом множина *M*, множина *O* в їх взаємозв'язку дають повний опис СЗДІ організації.

Ймовірності порушення достовірності в ІП визначаються, з одного боку, способами досягнення цілей, а з іншого - якістю засобів забезпечення достовірності. Загалом, достовірність інформації і інші показники якості будуть визначені при детальному розгляді всіх областей графа, при цьому ефективність характеризується співвідношенням ризиків від порушення достовірності інформації в ІП організації при відсутності і при наявності СЗДІ.

Отже, методика оцінки поточного рівня достовірності інформації як ймовірності збереження її незмінності в інформаційному потоці в умовах інформаційних впливів вимагає врахування: частоти виникнення факторів інформаційного протиборства, можливості порушення достовірності, ймовірності виявлення спроб порушення достовірності інформації. Інформаційний простір організації, підприємства, держави дуже часто складається з множини різнорідних компонентів, що не дає можливості одержувати числові компоненти статистичними методами. Відтак, найбільш доцільними тут є методи експертного оцінювання.

3.2. Розробка алгоритму експертизи достовірності інформації

В умовах різнорідності елементів і параметрів ІП і переважно якісного опису багатьох показників для визначення поточного рівня ДІ необхідна процедура експертизи, адекватна поставленому завданню. Внаслідок того, що оцінку поточного рівня достовірності необхідно проводити регулярно, а кількість параметрів ІП обчислюється сотнями, то такою процедурою є однотурова анонімна процедура на основі математичних методів, що дають

досить адекватне перетворення первинних результатів зі згладжуванням неузгодженостей оцінок експертів [102].

У загальний алгоритм проведення експертизи [103, 104] необхідно внести ряд змін і доповнень, орієнтованих на комплексний облік різних інформаційних впливів, що знижують ДІ. Нижче представлений у вигляді поділу на етапи доопрацьований таким чином алгоритм.

1) Формулювання мети експертизи та визначення її об'єктів.

Метою експертизи є оцінка кількісних і якісних параметрів ІП згідно моделі, представленої на рис. 3.1. при визначенні об'єктів проведення експертизи необхідно повною мірою враховувати організаційний, фізичний і програмно-технічний рівні забезпечення достовірності, але це не означає, що всі рівні стають рівнозначними: в залежності від конкретної структури інформаційних процесів (ІПр) в ІП і якості СЗДІ можуть виходити на перший план і чинити більший вплив на достовірність інформації СУ одного з рівнів.

2) Формування аналітичної групи.

Даний етап експертизи ІП не має будь-яких особливостей стосовно оцінки ДІ і проходить відомим чином [105, 106].

3) Затвердження складу експертної групи (ЕГ).

При формуванні ЕГ необхідно оцінити передбачувану ступінь компетентності експерта (коефіцієнт авторитету). існує ряд способів визначення коефіцієнтів авторитету на основі статистики попередніх експертиз [107]. При відсутності статистики, а також у разі участі експерта в першій своїй експертизі коефіцієнти авторитету можуть бути визначені на основі формальних відомостей про експертів і нормовані за умовою.

$$\sum_{\varepsilon=1}^{m} v_3^0 = 1. \qquad (3.5)$$

Можуть бути використані такі відомості про експертів:

A. Освіта;

B. Наукова підготовка;

C. Стаж роботи за пріоритетним напрямком;

D. Кількість проведених експертиз.

Оцінка може бути проведена з використанням шкали балів (табл. 3.1).

Кількість балів по пунктах A, B, C, D підсумовуємо і таким чином визначаємо первинний бал експерта B_3^0.

Коефіцієнт авторитету з урахуванням нормування обчислюємо за формулою

$$V_\varepsilon^0 = \frac{B_\varepsilon^0}{\sum_{\varepsilon=1}^{m} B_\varepsilon^0} \tag{3.6}$$

Таблиця 3.1

Шкала оцінки компетенстності експертів

Напрямок	Опис всередині напрямку	Бал
A	за пріоритетним напрямком	5
	за суміжною спеціальністю	4
	у напрямку (незакінчена)	3
	за суміжною спеціальністю (незакінчена)	2
	не співдапає з профілем експертизи	0
B	академік	5
	доктор наук	4
	кандидат наук	3
	аспірант, с.н.с.	2
	без степеню	0
C	Не меньше 10 років	5
	не менше 5 років	4
	не менше 1 року	3
	менше1 років	1
	Відсутнє	0
D	Більше 20	5
	10-20	4
	4-9	3
	1-3	1
	ні	0

При проведенні експертиз, звернення до експертів пов'язані з певними фінансовими витратами. З огляду на цю обставину, при формуванні експертної групи можна використовувати наступний метод [106].

Нехай *Ck* - умовна вартість звернення до *k*-му експерту, а *C* - гранична сумарна вартість звернення до всіх експертів. Нехай x_k = 1, якщо експерт включений в групу і $x_{k=0}$, якщо ні. Тоді задачу формування експертної групи, яка має максимальну компетентність, можна записати як задачу лінійного програмування наступним способом:

$$\begin{cases} \sum_k v_k x_k \ \rightarrow max, \\ \sum_k C_k x_k \ \leq \ C. \end{cases} \tag{3.7}$$

Коефіцієнт авторитету, визначений за (3.7) є первинним. Не завжди якість оцінок експерта відповідає формальним відомостями про нього. Первинний коефіцієнт повинен бути скоректований на основі узгодженості суджень експерта.

4) Підготовка необхідної інформації про об'єкти експертизи, її аналіз і систематизація.

При проведенні експертизи ІП найбільшу кількість часу буде витрачено на вивчення її характеристик, тому що необхідно розглянути два основних питання: призначення і принципи функціонування ІП і області СУ, ФІП, ІР, засобів СЗДІ. Обидва ці питання можуть бути дозволені в ході опитувань користувачів і розробників ІП, на що потрібні великі витрати часу.

Іншим джерелом інформації про об'єкт є проектна, робоча і експлуатаційна документація. Іноді якість документації буває низькою або вона просто відсутня. З іншого боку, там, де вона існує, її обсяг може

обчислюватися сотнями і тисячами сторінок друкованого тексту. Документація також може містити застарілі відомості.

Найбільш ефективним методом збору інформації про ІП є комплексний метод, при якому керівництво організації, що розробляє або експлуатує ІП, ставить перед її розробниками або іншим персоналом завдання підготувати таку інформацію і представити її в експертну групу.

Проведення експертизи ІП для оцінки поточного рівня ДІ вимагає наступних документів:

- документи, що містять вимоги безпеки,
- опису ІП,
- опис механізмів забезпечення достовірності.

5) Попереднє ознайомлення експертів з матеріалами про об'єкти експертизи, щоб отримати додаткову інформацію.

Часто після першого ознайомлення експертів з підготовленою документацією, яка описує об'єкт експертизи, у них виникають різні питання, які по можливості повинні бути усунені підготовкою додаткової інформації. Загалом це стосується більш детального опису інформаційних процесів та механізмів забезпечення достовірності.

6) Вибір процедури проведення експертизи.

Існує два принципи експертного оцінювання [108]. Відповідно до першого кожному об'єкту експертизи повинна бути дана оцінка загалом, у відповідності з другим - багатокритеріальна оцінка по кожному з критеріїв оціночної системи з подальшим автоматизованим розрахунком результуючої оцінки. Показники ДІ не є такими параметрами, які можна оцінити безпосередньо, таким чином перший принцип не підходить.

7) Визначення оціночної системи.

Оцінку кількісних параметрів можна реалізувати в шкалах у відповідності з фізичним змістом параметра [109]. У задачі оцінки рівня достовірності якісні параметри ІП можна умовно розділити на два типи:

- вимагають отримання абсолютного результату;
- вимагають отримання порівняльного результату (відносної значущості) в ряді альтернатив.

Оціночною величиною перших стає нечітка множина, функція приналежності якої показує розподіл можливості всіх передбачуваних результатів. Нормований розподіл значимості в повній множині альтернатив, отриманій на основі парних порівнянь з лінгвістичним таблиць, дає шуканий результат для параметрів другого типу.

9) Обробка первинних результатів експертизи.

Отримані первинні оцінки можуть бути якісними, тоді для отримання кількісного результату необхідно їх перетворення в кількісні значення за таблицями відповідності або з використанням баз знань. Крім того, оцінки параметрів, що мають різний фізичний зміст, дані в різних шкалах, отже, потрібно зведення оцінок в рамках єдиної моделі і отримання декількох загальних показників.

У зв'язку з неможливістю абсолютної формалізації отримання первинних оцінок судження експертів будуть розходитися. Ступінь такої розбіжності (або зворотний їй показник - ступінь узгодженості) показує якість отримання єдиної оцінки і служить для корекції коефіцієнтів авторитету експертів зі збільшенням коефіцієнтів експертів, що дали більш узгоджені оцінки, що дозволяє підвищити узгодженість всі експертизи в цілому.

10) Отримання результатів - показників якості ІП.

Розрахунок загального коефіцієнта достовірності інформації D_{IP} і економічної ефективності *Ef* проходить на основі процедур, розглянутих далі в цьому розділі.

11) Прийняття рішення за результатами експертизи.

Результати експертизи можуть бути визнані адекватними, тоді рішенням буде вироблення рекомендацій щодо вдосконалення СЗДІ з метою підвищення

ДІ в ІП, за умови, що СЗДІ економічно ефективна, або пропозиції по переробці СЗДІ, що є неефективною, за умови, що рівень ДІ недостатній.

Отже, через необхідність регулярної оцінки поточного рівня достовірності при значній кількості елементів інформаційного простору основною процедурою оцінювання є однотурова анонімна процедура на основі математичних методів згладжування неузгодженостей оцінок експертів. Оцінку кількісних параметрів найбільш доцільно реалізувати в шкалах у відповідності з фізичним змістом параметра. Отримані якісні оцінки перетворюються у кількісні значення за таблицями відповідності або з використанням баз знань, після чого оцінюються як кількісні параметри.

3.3. Розробка методики оцінки кількісних параметрів достовірності інформації

Оцінка чітких кількісних параметрів. Підмножина параметрів ІП визначені чітким кількісним значенням. Як приклади можна привести: «в локальну мережу відділу входить 4 робочі станції, один сервер, один принтер і один маршрутизатор »; «Кількість відомих вірусів в БД встановленого антивіруса - 83468»; «Період оновлення антивірусних баз - 1 місяць» і ін. Простановка первинних оцінок таких параметрів експертами не викликає складності, більш того, більшість з таких параметрів можуть бути визначені без власне експертизи на основі наявної документації. Такі оцінки є точковими значеннями на певній шкалі. Але виникає деяка проблема.

По-перше, в наведених вище прикладах можна відзначити три види одиниць виміру: безрозмірні, просторові і часові. Тобто виходить, що параметри потрібно оцінити за різними шкалами, при цьому всі вони впливають на ДІ і повинні бути зведені в єдину систему. По-друге, для всіх

параметрів можна вказати необхідне або оптимальне значення; і якщо перше можна якимось чином виділити зі стандартів, то для другого без експертизи не обійтися.

Розглянемо докладніше рішення першої сторони проблеми. У процесі проведення оцінки в залежності від фізичної природи оцінюваного параметра можуть бути використані різні шкали: шкала інтервалів, шкала відносин, шкала різниць, абсолютна шкала [106]. Параметри для оцінювання різнорідні і для їх спільного використання в одній моделі необхідно унормувати кількісні дані з урахуванням їх значущості. Нормування, зокрема, можна виконати зведенням до одиничного інтервалу дійсних чисел [0, 1] з урахуванням вагових коефіцієнтів при наступних перетвореннях. Адекватність вибору саме одиничного інтервалу обумовлена тим, що в тому ж інтервалі змінюються ймовірності і функція приналежності в теорії нечітких множин, і як кінцевий результат дослідження - достовірність інформації.

Для нормування необхідно ввести поняття «мінімальна», «максимальне», «найкраще», «найгірший» і «оптимальне» значення qго параметра. Позначимо їх X_q^{MIN}, X_q^{MAX}, $X_q^{НК}$, $X_q^{НГ}$, $X_q^{ОПТ}$. Мінімальним назвемо значення, найменше за величиною і досяжне в системі. Найчастіше за все це 0 (крім тимчасових параметрів). Максимальне значення визначається технічними характеристиками системи як «максимально досяжне» значення.

Очевидно, що не завжди максимальне значення є найкращим, а мінімальне - найгіршим. Зазвичай для всіх «позитивних» параметрів (як то кількість засобів забезпечення достовірності) максимальне - є найкраще, а для всіх «негативних» характеристик (Час виконання операції, кількість одиниць доступу і т.д.) максимальне - є найгірше. Крім того, можна відзначити, що не завжди екстремальне значення параметра оптимально з точки зору організації СЗДІ.

Для нормування можуть бути використані перетворення виду:

- якщо максимальне значення параметра є оптимальним, то

$$X_q^{MAX} \to X_q^{\text{НК}} = X_q^{\text{ОПТ}},\ X_q^{MIN} \to X_q^{\text{НГ}};\ \overline{X_q} = \frac{Xq - X_q^{Min}}{X_q^{Max} - X_q^{Min}}; \qquad (3.8)$$

- якщо мінімальне значення параметра є оптимальним, тобто

$$X_q^{MIN} \to X_q^{\text{НК}} = X_q^{\text{ОПТ}},\ X_q^{MAX} \to X_q^{\text{НГ}};\quad \overline{X_q} = \frac{X_q^{MAX} - X_q}{X_q^{MAX} - X_q^{MIN}}; \qquad (3.9)$$

- якщо оптимальне значення параметра знаходиться між мінімальним і максимальним, які обидва є найгіршими, то

$$X_q^{\text{НК}} = X_q^{\text{ОПТ}},\ X_q^{MIN} \to X_q^{\text{НГ}},\ X_q^{MAX} \to X_q^{\text{НГ}},\ X_q^{MIN} \le X_q^{\text{ОПТ}} \le X_q^{MAX},$$

$$\bar{X}_q = \begin{cases} 0, X_q = X_q^{MIH} \text{ або } X_q = X_q^{MAX} \\ 1, \qquad X_q = X_q^{\text{ОПТ}} \\ \frac{X_q - X_q^{\text{МІН}}}{X_q^{\text{ОПТ}} - X_q^{MIN}}, X_q^{MIN} < X_q < X_q^{\text{ОПТ}} \\ \frac{X_q^{MAX} - X_q}{X_q^{MAX} - X_q^{\text{ОПТ}}}, X_q^{\text{ОПТ}} < X_q < X_q^{MAX} \end{cases} \qquad (3.10)$$

Оцінка нечітких кількісних параметрів. Якщо в якості оптимального значення неможливо використовувати статистично певну величину, або взяту з стандарту [106, 110], то таке значення є суб'єктивною величиною, яка знаходиться експертним шляхом. Отже, вона може бути представлена нечітким числом з трикутною (можливо, несиметричною) функцією приналежності.

При визначенні оптимального значення кількісного вимоги кожен експерт представляє свої оцінки у вигляді трійки чисел

$$\langle a_\varepsilon, X_\varepsilon^{\text{ОПТ}}, b_\varepsilon \rangle, \qquad (3.11)$$

де $X_\varepsilon^{ОПТ}$ мода (точне значення нечіткого числа) - передбачуване експертом оптимальне значення параметра, a_ε і b_ε задають лівий і правий кордон нечіткості, тобто величини, за межами яких значення параметра експерт з абсолютною впевненістю рахує не оптимальним.

Оцінки всіх експертів можна представити графічно на рис. 3.3

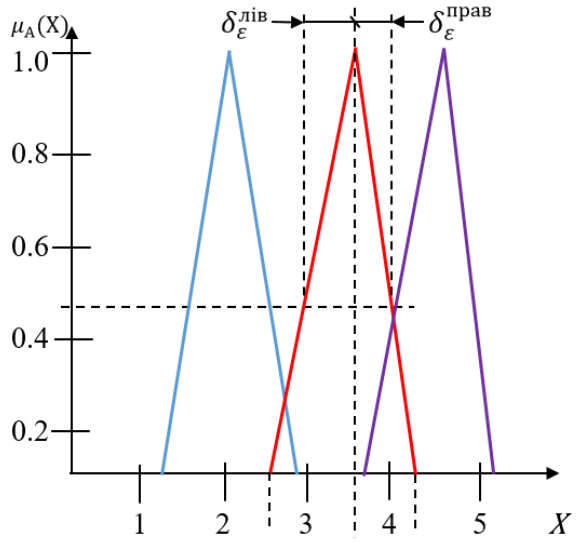

Рис. 3.3. Оцінки ряду експертів оптимального значення параметра

Величини $\delta_\varepsilon^{Лів}$ і $\delta_\varepsilon^{Прав}$ визначають ліве і праве відхилення для α-зрізу 0,5, тобто значення при яких експерт називає значення оптимальним з упевненістю 0,5.

Очевидно, що:

$$\delta_\varepsilon^{Лів} = a_\varepsilon + \frac{X_\varepsilon^{ОПТ} - a_\varepsilon}{2},\ \delta_\varepsilon^{Прав} = b_\varepsilon + \frac{X_\varepsilon^{ОПТ} - b_\varepsilon}{2}. \qquad (3.12)$$

Розрахунок значень параметра $\delta^{Лів}$, $\delta^{Прав}$, $X^{ОПТ}$ можливий з урахуванням уточненого коефіцієнта авторитету.

$$\delta_{\text{Лів}} = \sum_{\varepsilon=1}^{m} \delta_{\varepsilon}^{\text{Лів}} * v_{\varepsilon},$$
$$\delta_{\text{Прав}} = \sum_{\varepsilon=1}^{m} \delta_{\varepsilon}^{\text{Справ}} * v_{\varepsilon},$$
$$X^{\text{ОПТ}} = \sum_{\varepsilon=1}^{m} X_{\varepsilon}^{\text{ОПТ}} * v_{\varepsilon} \quad (3.13)$$

де v_{ε} - коефіцієнт авторитету ε-го експерта.

Опис нечіткого кількісного параметра відповідає виразу «приблизно <значення z>», тобто має нормальний вигляд функції розподілу. Оцінка ступеня відповідності значення z_q опису може бути отримана наступним чином:

$$\bar{X}_q = \begin{cases} e^{-b_{\text{лів}}(z_q^{\text{ОПТ}} - z_q)^2}, & z_q \leq z_q^{\text{ОПТ}}, \\ e^{-b_{\text{прав}}(z_q^{\text{ОПТ}} - z_q)^2}, & z_q \leq z_q^{\text{ОПТ}}, \end{cases} \quad (3.14)$$

де β залежить від необхідного ступеня нечіткості і визначено з

$$\beta_{\text{лів}} = \frac{\ln a}{4\delta_{\text{лів}}^2}$$
$$\beta_{\text{прав}} = \frac{\ln a}{4\delta_{\text{прав}}^2} \quad (3.15)$$

де $\delta_{\text{лів}} + \delta_{\text{прав}}$ визначає відстань між точками переходу для функції приналежності (3.13), тобто точками, в яких функція приймає значення α зі ступенем впевненості 0.5.

Рівень α визначає ступінь допущення приналежності реального значення параметру z_Q потрібному $z_q^{\text{потр}}$, або оптимальному $z_q^{\text{ОПТ}}$. Зазвичай $\alpha \in [0{,}5, 1{,}0]$.

Рис. 3.4 ілюструє співвідношення між даними величинами.

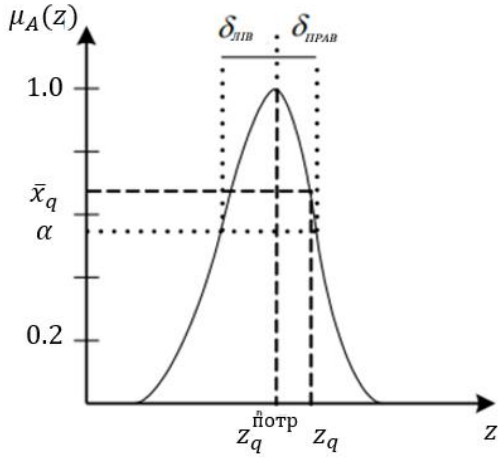

Рис. 3.4. Графічне представлення функції приналежності якісного опису кількісного параметра.

Отже, чіткі кількісні параметри оцінюються або в абсолютних величинах, або в нормованих відповідно до обраної шкали нормування. У якості шкал використовуються шкала інтервалів, шкала відносин, шкала різниць або абсолютна шкала. Нечіткі кількісні параметри оцінюються, як правило, за нечітким числом з трикутною (симетричною чи несиметричною) функцією приналежності. При цьому експерти представляють свої оцінки у вигляді трійки чисел. За необхідності, точність оцінювання може бути підвищена шляхом використання уточнюючого коефіцієнта авторитету.

3.4. Розробка алгоритмів оцінювання якісних параметрів достовірності інформації

У процесі проведення експертизи експертові доводиться стикатися з якісними параметрами або їх описами. У задачі оцінки ДІ необхідно досліджувати ймовірності виникнення, виявлення та усунення помилок, які визначаються деякими числовими значеннями. У той же час ряд СУ різних

елементів ІП характеризується спочатку якісними описами. Наприклад, помилки персоналу під час експлуатації ІП залежать від якості посадових інструкцій, контролю з боку керівників, розподілу обов'язків та організації праці. Це призводить до виникнення проблеми переходу від якісних описів до кількісних значень.

Всі якісні параметри можна розділити на ті, які мають точний опис, тобто існує або може бути задана послідовність описів, упорядкованих по рангової шкалою [106], і ті, які не мають такого ряду описів (зокрема, якісні вимоги різних стандартів).

Приклади параметрів, які можна описати за рангової шкалою:

- «значимість деякого, об'єкта, події, умови»;
- «доступність, простота використання будь-якого методу або засоби";
- «цінність ресурсу (відносна)»;
- «ступінь впливу деякого умови на прояв події»

Перераховані параметри можуть бути оцінені шляхом використання прямого перетворення по лінгвістичним таблицями [111] або за допомогою парних порівнянь альтернатив. На відміну від кількісних, оцінка якісних параметрів однією людиною зазвичай дає неадекватний результат. Робота експертної групи з достатньою кількістю експертів дозволяє підвищити якість оцінки. Алгоритм отримання експертних оцінок якісних параметрів з реалізацією многотурових анонімних процедур представлена на рис. 3.5.

Рис. 3.5. Алгоритм отримання експертних оцінок якісних параметрів

якості питань, поставлених перед експертом. Чіткі питання ускладнюють задачу аналітичної групи, яка їх готує і обробляє результати. Більш абстрактні питання ускладнюють задачу експерта і можуть привести до отримання неадекватного результату або результатів з більшій ступені неузгодженості. Таким чином, найбільш значущою проблемою є формалізація процесу підготовки питань і проведення експертизи [112].

Більшість нечислових характеристик можна описати за рівневою шкалою, використовуючи поняття «високий», «середній» і «низький» рівні. В даному випадку питання перед експертом поставлено чітке. Але експерт за такою шкалою присвоїть один і той же, наприклад, «середній рівень» кількома параметрами, які мають насправді відмінні риси, які не можна просто так усереднити.

Якщо істотно збільшити кількість рівнів шкали, то тоді може виникнути ситуація, при якій експерту буде важко вибрати найбільш підходящий. І не для

всіх характеристик можна придумати більш трьох рівнів. Людині завжди простіше виконати порівняння двох об'єктів, ніж дати вичерпну характеристику кожному окремо. Отже, адекватна оцінка може бути дана шляхом парних порівнянь альтернатив.

У задачі оцінки поточного рівня ДІ в ІП одним з якісних параметрів є значимість ряду елементів або умов для виникнення деякої події [113].

Алгоритм оцінки значимості умов. Одним із прикладів такої характеристики є «значущості ряду СУ для виникнення помилки, що приводить до зниження вірогідності оброблюваної інформації» [114].

Алгоритм представлений на рис. 3.6.

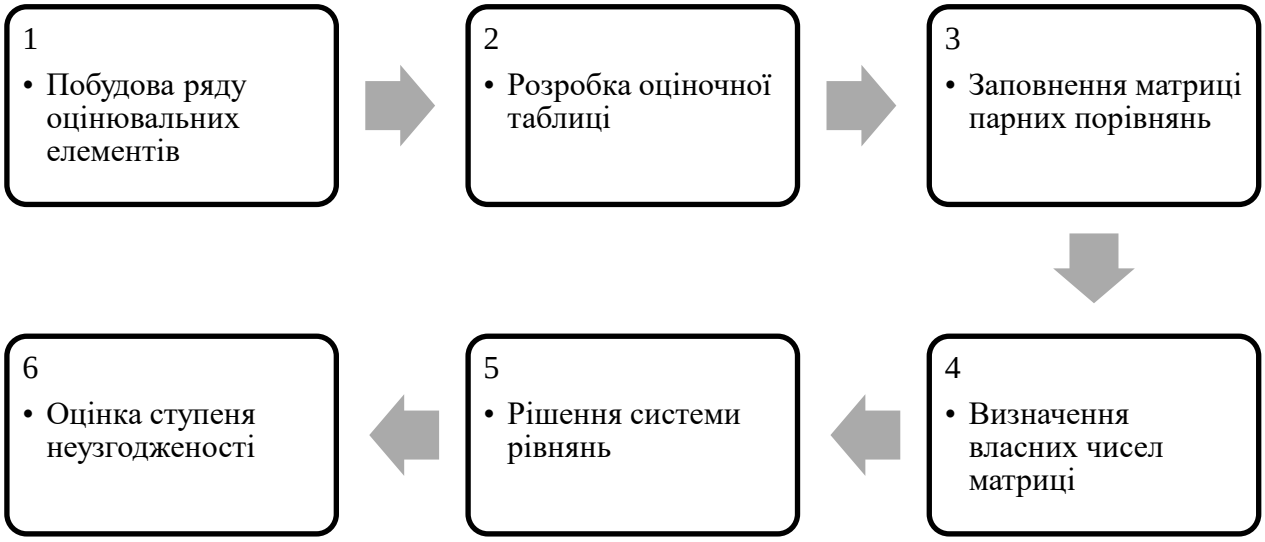

Рис . 3.6. Алгоритм визначення значущості умов для виникнення події.

На першому етапі формуємо множину оцінюваних елементів $E = \{ e_1 , e_2 , ... e_n \}$.

Другий етап полягає в розробці лінгвістичних описів, тобто варіантів оцінки елемента і присвоєння їм числових значень, які можуть бути взяті, наприклад, за методом Сааті як натуральні числа $\{1,2, ..., 9\}$ [100, 115]. Але

типова таблиця лінгвістичних описів як правило, мало інформативна. Тому для різних параметрів на її базі повинні бути розроблені більш конкретні опису. Вони дані в табл. 3.2-3.6.

Для тих параметрів, визначення значимості яких можливо безпосередньо (без парних порівнянь), використовуємо той же діапазон значень, але вже не в шкалі відносної значущості, а в рангової шкалою.

Для програмно-апаратного і організаційного типу СУ можна уточнити формулювання табл. 3.3. Один з варіантів представлений в табл. 3.4 і 3.5.

Таблиця 3.2

Значимість СУ (за шкалою відносної значущості)

Лінгвістична оцінка порівняння 1-го и 2-го СУ	Значення
При наявності 1-го СУ наявність 2-го можна не враховувати	9
Істотну перевагу значущості 1-го СУ над 2-м	7
Використання 1-го СУ краще, ніж 2-го	5
Трохи більш висока значимість 1-го СУ проти 2-го	3
Однакова значимість порівнюваних СУ	1

Таблиця 3.3

Доступність СУ (по рангової шкалою)

Лінгвістична оцінка	Значення
СУ є загальновідомим, для його використання не потрібно спецзасобів і особливих здібностей	9
СУ є загальновідомим, але для його використання потрібні від-носительно доступні технічні засоби	7
СУ поширений, для його використання потрібні дорогі або широко недоступні спецзасоби	5
СУ є маловідомим і / або для його використання потрібні дорогі або широко недоступні спецзасоби, ресурси, заходиі т.д.	3
Використання СУ вимагає таких ресурсів і засобів, які застосувати приховано неможливо або їх застосування вимагає величезних витрат часу.	1

Таблиця 3.4

Доступність СУ програмно-апаратного рівня

Лінгвістична оцінка	Значення
СУ відомий, для його використання не потрібно спеціальних вичісненістю потужностей, програмних засобів, великого ресурсу часу і грошових витрат	9
Потрібні типові програмно-апаратні засоби, можливо з невеликими витратами часу	7
СУ маловідомий (для його використання потрібно спеціальні знання і навички), істотні грошові витрати, спеціальне обладнання та / або ресурси часу	5
СУ є маловідомим, для його використання потрібні спеціальні знання і обладнання, великі обчислювальні потужності, су- суспільних грошові витрати	3
Для використання СУ потрібно обладнання спецслужб і / або ви- числівники потужності супер-комп'ютерів, а також великі витрати і / або ресурси часу	1

Таблиця 3.5

Доступність СУ організаційного плану

Лінгвістична оцінка	Значення
СУ відомий широкому колу осіб, не вимагає спецзасобів, підготовки і проникнення в АСУП.	9
СУ відомий широкому колу осіб, не вимагає проникнення в АСУП, але вимагає щодо доступних спеціальних засобів	8
СУ відомий широкому колу осіб, для його використання потрібні відносно доступні спеціальні засоби, проникнення в АСУП або додаткова підготовка.	7
СУ відомий широкому колу осіб, для його використання потрібні відносно доступні спеціальні засоби, проникнення в АСУП і додаткова підготовка протягом тривалого часу.	5
СУ маловідомий, для його використання потрібні дорогі або мало- доступні спецзасоби, проникнення в АСУП і додаткова підприготування протягом тривалого часу.	3
СУ маловідомий, для його використання потрібні значні за- витрати ресурсів і тривала підготовка, проникнення в АСУП сопряжено зі значними складнощами.	1

Таблиця 3.6

Цінність ІР (по рангової шкалою)

Лінгвістична оцінка цінності ІР на основі розрахунку витрат на відновлення	Значення
Даний ІР є найважливішим для організації. Його втрата завдасть непоправні наслідки для організації.	9
Витрати на ліквідацію наслідків через втрату ресурсу можна порівняти з річними економічними показниками	8
Витрати на відновлення через втрату ресурсу істотні для організації	6
Витрати на відновлення несуттєві, але потрібний додатковий час	2
Відновлення через втрату ресурсу буде проведено в штатному режимі	1

На третьому етапі експерт заповнює матрицю парних порівнянь для кожної пари елементів.

$$\mathrm{M}_{\varepsilon}^{\mathrm{A}} = \begin{bmatrix} a_{11}^{\varepsilon} & a_{12}^{\varepsilon} & \dots & a_{1n}^{\varepsilon} \\ a_{21}^{\varepsilon} & a_{22}^{\varepsilon} & \dots & a_{2n}^{\varepsilon} \\ a_{n1}^{\varepsilon} & a_{n1}^{\varepsilon} & \dots & a_{nn}^{\varepsilon} \end{bmatrix} \qquad (3.16)$$

де $A=\{a_1, a_2, ..., a_n\}$ - множина параметрів, $a_{\alpha\beta}$ - опис відносин, взятий з таблиці 3.2, $\varepsilon \in \{1, 2, ..., m\}$ - номер експерта.

Матриця (3.16) є обернено симетричною, тобто для кожної пари елементів виконується умова:

$$a_{\alpha\beta}^{\varepsilon}=\frac{1}{a_{\beta\alpha}^{\varepsilon}},\ \forall \alpha\ \beta=\overline{1,n},\ \forall\ \varepsilon=\overline{1,m}. \qquad (3.17)$$

Таким чином, експерт визначає тільки значення елементів матриці вище (або навпаки нижче) головної діагоналі. При цьому кількість порівнюваних елементів визначаємо за формулою

$$KC = \frac{n(n-1)}{2}. \quad (3.18)$$

Елементарний аналіз цієї залежності кількості порівнянь від розмірності матриці показує, що при n від 20-30 і вище кількість порівнянь стає занадто великим (від 200 і більше - і це тільки по одному параметру), що ставить перед експертом практично не здійсненне завдання.

У процесі порівняння виникає ще одна парадоксальна ситуація: ті ж СУ (і інші характеристики) розділені на категорії за типом (Наприклад, технічні, програмні, апаратні та організаційні СУ). Адекватно порівняти різнорідні характеристики просто неможливо.

Запропоновано наступний метод оцінки в умовах розглянутої ситуації. Припустимо, що виділені дві групи порівнюваних альтернатив (даний метод може бути легко поширений на будь-яку кількість груп). Для кожної групи необхідно побудувати окремі матриці типу (3.16), але зі зміненим умовою (3.17).

$$M_{\varepsilon}^{Br} = \begin{vmatrix} br_{11}^{\varepsilon} & br_{12}^{\varepsilon} & \dots & br_{1k_r}^{\varepsilon} \\ br_{21}^{\varepsilon} & br_{22}^{\varepsilon} & \dots & br_{2k_r}^{\varepsilon} \\ \dots & \dots & \dots & \dots \\ br_{k_r1}^{\varepsilon} & br_{k_r2}^{\varepsilon} & \dots & br_{k_rk_r}^{\varepsilon} \end{vmatrix} \quad (3.19)$$

де $Br = \{br_1, br_r, \dots br_{k1}\}$ - множина параметрів r-групи з k_r- параметрів;

всього l груп, $br_{\alpha\beta} = a_{\alpha\beta} - 1$, $\forall r$ - ($a_{\alpha\beta} \geq 1$ взято з таблиці 3.2), $\varepsilon \in \{1, 2, \dots, m\}$ – номер експерта;

нова умова наступна:

$$br_{\alpha\beta}^{\varepsilon} = - br_{\beta\alpha}^{\varepsilon}, \forall \alpha, \beta = \overline{1, k_r}, \forall \varepsilon = \overline{1, m}, \ \forall r = \overline{1, l} \quad (3.20)$$

Далі експерт дає парне порівняння значущості кожної групи по умові аналогічно (3.20)

$$M_{\varepsilon}^{r} = \begin{vmatrix} r_{11}^{\varepsilon} & r_{12}^{\varepsilon} & \dots & r_{1\mathrm{I}}^{\varepsilon} \\ r_{21}^{\varepsilon} & r_{22}^{\varepsilon} & \dots & r_{2\mathrm{I}}^{\varepsilon} \\ \dots & \dots & \dots & \dots \\ r_{\mathrm{I}1}^{\varepsilon} & r_{\mathrm{I}2}^{\varepsilon} & \dots & r_{\mathrm{II}}^{\varepsilon} \end{vmatrix} \tag{3.21}$$

Потім в загальну матрицю вносимо часткові оцінки кожної групи. Для двох груп вона буде виглядати наступним чином:

$$M_{\varepsilon}^{B} = \left|\begin{array}{ccc|ccc} b1_{11}^{\varepsilon} & \cdots & b1_{1k_1}^{\varepsilon} & & & \\ \cdots & \cdots & \cdots & & & \\ b1_{k_1 1}^{\varepsilon} & \cdots & b1_{k_1 k_1}^{\varepsilon} & & & \\ \hline & & & b2_{11}^{\varepsilon} & \cdots & b2_{1k_2}^{\varepsilon} \\ & & & \cdots & \cdots & \cdots \\ & & & b2_{k_2 1}^{\varepsilon} & \cdots & b2_{k_2 k_2}^{\varepsilon} \end{array}\right| \tag{3.22}$$

Залишається заповнити позиції порівняння елементів з різних груп на основі (3.21), що може бути зроблено в автоматизованому режимі без участі експерта.

Загальна картина порівняння всіх елементів, скажімо, 1-ї і 2-ї групи визначається величиною $\Gamma_{12}^{\varepsilon}$, яка не відображає відносини кожної окремої пари елементів.

Розглянемо будь-який рядок матриці (3.19). Величина $br_{\alpha\beta}^{\varepsilon}$ відображає порівняльну характеристику α - і β-елементів, яке за умови (3.20) можна вважати зміщенням по шкалі рангів.

Сума $Sbr_{\alpha}^{\varepsilon} = \sum_{\beta=1}^{k_r} br_{\alpha\beta}^{\varepsilon}$, $(\forall\alpha = \overline{1, k_r}, \forall \mathrm{r} = \overline{1, \mathrm{l}}, \forall\varepsilon = \overline{1, \mathrm{m}})$ показує суму зсувів α -елементів щодо всіх $\beta = \overline{1, k_r}$ тобто по суті , його перевага, якщо сума

позитивна, придушення, якщо вона негативна і рівну значущість, якщо дорівнює нулю.

Очевидно, що з умови (3.20)

$$\sum_{\alpha=1}^{k_r} Sbr_{\alpha}^{\varepsilon}=0 \ (\forall \mathrm{r} = \overline{1,\mathrm{l}}, \forall \varepsilon = \overline{1,\mathrm{m}}). \qquad (3.23)$$

Таким чином, в поки незаповнені місця матриці (3.22) необхідно внести величини, рівні: сума рангів з рядка 1-й порівнюєш групи + сума рангів з колонки 2-ї групи + ранг порівняння груп в цілому.

Для двох груп параметрів заповнена матриця буде мати вигляд

$$M_{\varepsilon}^{B} = \left|\begin{array}{ccc|ccc} & & & Sb1_{1\_}^{\varepsilon}+Sb2_{\_1}^{\varepsilon}+ & & Sb1_{1\_}^{\varepsilon}+Sb2_{\_k_2}^{\varepsilon}+ \\ b1_{11}^{\varepsilon} & \cdots & b1_{1k_1}^{\varepsilon} & +\mathrm{r}_{12}^{\varepsilon} & \cdots & +\mathrm{r}_{12}^{\varepsilon} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ b1_{k_1 1}^{\varepsilon} & \cdots & b1_{k_1 k_1}^{\varepsilon} & Sb1_{k1\_}^{\varepsilon}+Sb2_{\_1}^{\varepsilon}+ & & Sb1_{k1\_}^{\varepsilon}+Sb2_{\_k2}^{\varepsilon}+ \\ & & & +\mathrm{r}_{12}^{\varepsilon} & \cdots & +\mathrm{r}_{12}^{\varepsilon} \\ \hline Sb1_{\_1}^{\varepsilon}+Sb2_{1\_}^{\varepsilon}+ & & Sb1_{\_k1}^{\varepsilon}+Sb2_{1\_}^{\varepsilon}+ & & & \\ +\mathrm{r}_{21}^{j} & \cdots & +\mathrm{r}_{21}^{j} & b2_{11}^{\varepsilon} & \cdots & b2_{1k_2}^{\varepsilon} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ Sb1_{\_1}^{\varepsilon}+Sb2_{k_2\_}^{\varepsilon}+ & & Sb1_{\_k_1}^{\varepsilon}+Sb2_{k_2\_}^{\varepsilon}+ & b2_{k_2 1}^{\varepsilon} & \cdots & b2_{k_2 k_2}^{\varepsilon} \\ +\mathrm{r}_{21}^{j} & \cdots & +\mathrm{r}_{21}^{j} & & & \end{array}\right| \qquad (3.24)$$

Для додаткового пояснення на рис. 3.7 показано формування окремих доданків в матриці (3.24).

Матриця (3.24) може містити не нормалізовані значення, а саме можливо таке, що $Sbr_{\alpha}^{\varepsilon}+Sbr_{\beta}^{\varepsilon}+\Gamma_{ab}^{\varepsilon}>8$ або $Sbr_{\alpha}^{\varepsilon}+Sbr_{\beta}^{\varepsilon}+\Gamma_{ab}^{\varepsilon}<-8$ тобто значення після зворотного перетворення вийдуть за межі шкали Сааті.

Нормалізація задається формулою

$$\bar{b}_{\alpha\beta} = \begin{cases} b_{\alpha\beta}, -8 \le b_{\alpha\beta} \le 8 \\ 8, \quad b_{\alpha\beta} > 8, \\ -8, \quad b_{\alpha\beta} < -8 \end{cases}, (\forall \alpha, \beta = \overline{1,n}). \qquad (3.25)$$

Нормалізована по (3.25) матриця (3.24) набуде вигляду

$$\bar{M}_{\varepsilon}^{B} = \begin{vmatrix} \bar{b}_{11}^{\varepsilon} & \bar{b}_{12}^{\varepsilon} & \dots & \bar{b}_{1n}^{\varepsilon} \\ \bar{b}_{21}^{\varepsilon} & \bar{b}_{22}^{\varepsilon} & \dots & \bar{b}_{2n}^{\varepsilon} \\ \dots & \dots & \dots & \dots \\ \bar{b}_{n1}^{\varepsilon} & \bar{b}_{n2}^{\varepsilon} & \dots & \bar{b}_{nn}^{\varepsilon} \end{vmatrix} \tag{3.26}$$

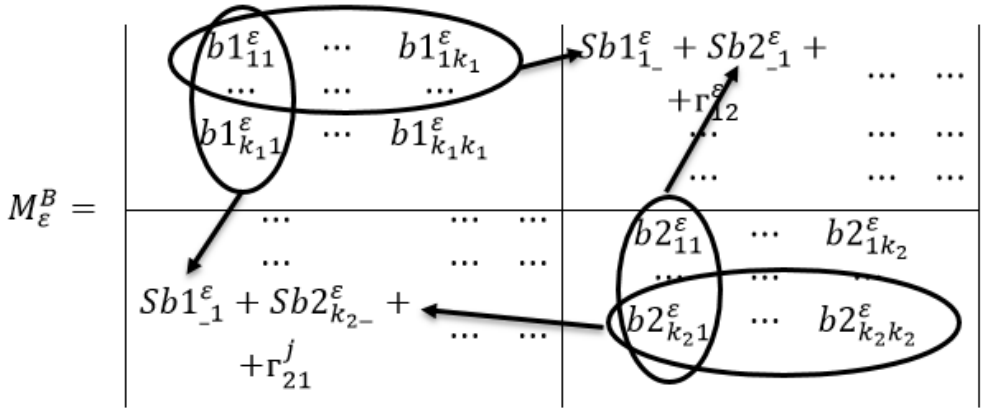

Рис. 3.7. Пояснення формування матриці (3.24)

Потім з матриці (3.26) необхідно отримати матрицю типу 3.16, використовуючи перетворення виду

$$a_{\alpha\beta} = \begin{cases} \bar{b}_{\alpha\beta} + 1, \bar{b}_{\alpha\beta} \geq 0 \\ \frac{1}{1-\bar{b}_{\alpha\beta}}, \bar{b}_{\alpha\beta} < 0 \end{cases} \tag{3.27}$$

Всі перетворення (3.22) - (3.27) можуть бути виконані програмно. Безсумнівним плюсом запропонованого підходу є значне зниження кількості порівнянь, яке максимально при однаковій кількості параметрів в кожній групі і так само

$$KC = l\frac{\frac{n}{l}*\frac{n-1}{l}}{2} + \frac{l(l-1)}{2} \approx \frac{n(n-1)}{2!} \tag{3.28}$$

тобто може бути зменшено майже в таке число раз, скільки виділено груп.

Несуттєвим недоліком підходу є необхідність будувати матриці порівняльної значимості окремих груп (3.21). якщо це робити один раз, і застосовувати для оцінки до всіх ФІП, то такий підхід дещо не достовірний (наприклад, для прояву одних ФІП можуть бути більш значущі програмні СУ, а для інших - фізичні).

Для поліпшення якості оцінки можливо будувати матриці (3.21) (а їх розмірність дорівнює числу груп, тобто відносно невелика) окремо для кожного типу ФІП.

На четвертому етапі необхідно визначити власні значення матриці (3.16) і власний вектор

$$A = \{ x_i^{\varepsilon} \}, \mathrm{i} = \overline{1, n}, \varepsilon = \overline{1, m}, \tag{3.29}$$

відповідний максимальному власному значенню $\lambda_{\max}^{\varepsilon}$ оцінок ε-го експерта.

Дана матриця є позитивно визначеною, обернено симетричною і визначення власного вектора на п'ятому етапі можливо методом Гаусса.

На шостому етапі проводиться дослідження якості оцінки. При проведенні порівнянь в реальній ситуації обчислене максимальне власне число $\lambda_{\max}^{\varepsilon}$ буде відрізнятися від відповідного власного числа λ_{max} для ідеальної матриці, внаслідок порушення її транзитивності (експерту надзвичайно складно проводити всі нові парні порівняння з урахуванням попередніх). Знайдені значення тим точніше, ніж ближче $\lambda_{\max}^{\varepsilon}$ до n. Причому завжди $\lambda_{\max}^{\varepsilon} \geq n$. Різниця $\lambda_{\max}^{\varepsilon} - n$ дає абсолютну міру неузгодженості оцінок. Відносна міра (коефіцієнт неузгодженості)

$$K_p^{\varepsilon} = \frac{\lambda_{\max}^{\varepsilon} - n}{n-1} \tag{3.30}$$

може бути використана для корекції коефіцієнта авторитету ε-го експерта.

Для такої корекції обчислюємо середній коефіцієнт неузгодженості

$$K_{CP}^{\varepsilon} = \frac{1}{k}\sum_{i=1}^{k} K_{\mathrm{Pi}}^{\varepsilon}, \qquad (3.31)$$

де k - кількість матриць парних порівнянь, побудованих експертом;

$K_{\mathrm{Pi}}^{\varepsilon}$ - коефіцієнт неузгодженості і-й матриці, обчислений за (3.30).

Обчислюємо уточнення коефіцієнта авторитету:

$$\Delta v_{\varepsilon} = \frac{1}{2}\left(v_{\varepsilon}^{0} + \frac{v_{\varepsilon}^{0}}{\sqrt{K_{CP}^{\varepsilon}}}\right). \qquad (3.32)$$

Уточнення передбачає, що виправлений коефіцієнт буде середнім арифметичним первинного коефіцієнта і його зниження через неузгодженості оцінок. Таке зниження буде різним у всіх експертів.

Скоригований коефіцієнт, що задовольняє правилу нормування, визначаємо за формулою

$$v_{\varepsilon} = \frac{\Delta v_{\varepsilon}}{\sum_{\varepsilon=1}^{m} \Delta v_{\varepsilon}}. \qquad (3.33)$$

Таким чином, для оцінки якісних параметрів необхідно спочатку розділити їх на ті, які мають точний опис, тобто існує або може бути задана послідовність описів, упорядкованих за ранговою шкалою. Такі параметри можуть бути оцінені шляхом використання прямого перетворення по лінгвістичним таблицям або за допомогою парних порівнянь альтернатив. Оцінка якісних параметрів передбачає на першому етапі оцінку значимості умов, зокрема структурно-функціональних недоліків інформаційної взаємодії.

На другому етапі здійснюється лінгвістичний опис варіантів оцінки елемента і присвоєння їм числових значень. Одержані оцінки заносяться у матрицю часткових оцінок, яка для декількох груп експертів буде мати блочний вигляд. Порівняння альтернатив здійснюється за сумою рангів рядків матриці за відповідними групами. Перевагою такого підходу є значне зниження кількості порівнянь. Крім того, запропонований підхід дозволяє враховувати авторитетність окремого експерта та неузгодженість думок експертів під час оцінювання.

3.5. Узагальнення моделі оцінки ризиків порушення достовірності інформації

Порушення достовірності інформації несе в собі ризики для підприємств, організацій, чи, у випадку державних інформаційних ресурсів, для держави. Оцінювання таких ризиків являє собою достатньо складне завдання. Розглянемо підхід щодо оцінювання та нейтралізації ризику, пов’язаного з впливом ФІП.

Нехай існує скінчена множина ФІП, які характеризуються відносними частотами виникнення $p_l^{\text{ФІП}}$ і збитком, що наноситься підприємству u_l , де $l = \overline{1,n}$. СЗДІ виконує функцію протидії порушення достовірності ІР. Основною характеристикою засобу забезпечення достовірності є можливість збереження достовірності ІР кожного *i*-го ІР при впливі на нього *l*-го ФІП p_{il}^{c}, яка пов'язана з можливістю порушення достовірності $p_{il}^{\text{НД}}$ через співвідношення

$$p_{il}^{c}=1-p_{il}^{\text{НД}}. \qquad (3.34)$$

Збиток ІП при відсутності СЗДІ може бути представлений як сумарний по кожному ФІП [95, 116, 120]

$$U=\sum_{l=1}^{n} U_l \tag{3.35}$$

У свою чергу залишковий збиток (тобто збиток, який все одно буде завдано ІП навіть при наявності СЗДІ - зловмисником можуть бути використані нові способи і засоби порушення достовірності) також є сумою втрат від всіх ФІП.

$$W=\sum_{l=1}^{n} w_l \tag{3.36}$$

Ризик для ІП при відсутності СЗДІ являє собою функцію відносних частот виникнення ФІП і збитку в разі порушення достовірності

$$R^{\text{НЗ}} = f(p_l^{\text{ФІП}}, u_i)=\sum_{l=1}^{n} p_l^{\text{ФІП}} * u_i \ , \tag{3.37}$$

а ризик для ІП при наявності СЗДІ залежить також і від можливостей збереження достовірності ІР

$$R^{\text{ЗАХ}} = f\left(p_l^{\text{ФІП}}, u_l, p_l^{c}\right) = \sum_{l=1}^{n} p_l^{\text{ФІП}} * \ u_l \ * \left(1 - \ p_l^{c}\right). \tag{3.38}$$

З огляду на імовірнісний характер ФІП, можна замінити відвернений збиток $\Delta W=U-W$ на усунутий ризик $\Delta R=R^{\text{НЗ}} - R^{\text{ЗАХ}}$ [119]. Тоді економічна ефективність функціонування СЗДІ може бути визначена як

$$\text{Ef}=\frac{R^{\text{НЗ}}-R^{\text{ЗАХ}}}{S_{\text{СЗД}}}=\frac{\sum_{l=1}^{n}p_l^{\text{ФІП}}*u_l*\sum_{l=1}^{n}p_l^{\text{ФІП}}*u_l*\left(1-p_l^{C}\right).}{S_{\text{СЗД}}} \qquad (3.39)$$

Для розрахунку економічної ефективності необхідно визначити перелік ІР і їх вартість, а також провести експертизу таких параметрів ІП, як значущості та доступності СУ і ступінь впливу кожного ФІП на все ІР ІП. Достовірна експертиза параметрів ІП можлива тільки на основі визначення повного списку актуальних ФІП та СУ, за умови адекватної оцінки ступеня виконання кількісних і якісних вимог до СЗДІ.

Збиток від порушення достовірності інформації. Розглянемо методи, що застосовуються для оцінки збитку від порушення достовірності ІР.

Збиток u_{i} , що наноситься ІП *l*-м ФІП за відсутності СЗДІ, може бути визначений в абсолютних одиницях: економічні втрати, тимчасових витратах, обсязі знищеної або "зіпсованої" інформації і т.д. [112].

Збиток від порушення достовірності ІР - це функція двох параметрів: ступінь впливу *l*-го ФІП на *i*-й ІР і вартість ресурсу $S_{\text{IP i}}$.

Ступінь впливу повинна бути визначена експертним шляхом по лінгвістичній таблиці і внесена в матрицю

$$M_{\varepsilon}^{H}=\begin{vmatrix} h_{11}^{\varepsilon} & h_{12}^{\varepsilon} & \dots & h_{1\text{I}}^{\varepsilon} \\ h_{21}^{\varepsilon} & h_{22}^{\varepsilon} & \dots & h_{2\text{I}}^{\varepsilon} \\ \dots & \dots & \dots & \dots \\ h_{n1}^{\varepsilon} & h_{n2}^{\varepsilon} & \dots & h_{nz}^{\varepsilon} \end{vmatrix} \qquad (3.40)$$

де $0\leq h_{ik}^{\varepsilon}\leq 1$ показує ступінь впливу *l*-го ФІП на *i*-й ІР.

$Sh_i^{\varepsilon}=\sum_{l=1}^{n}h_{li}^{\varepsilon}$, $\forall \text{i}=\overline{1,\text{z}}$, $\forall\varepsilon=\overline{1,\text{m}}$ показує сумарний збиток для *i*-го ІР і не повинна бути більше $Sh_{\text{Ир i}}$. Але при досить великій кількості ФІП та їх вплив на множину ресурсів таку умову може бути порушено. Тоді стовпчики матриці (3.37) необхідно масштабувати:

$$\bar{h}_{li}=\begin{cases} h_{li}, & Sh_i \le S_{\text{IP.i}} \\ h_{li} * \frac{S_{\text{IP.i}}}{Sh_i}, & Sh_i > S_{\text{IP.i}}, \end{cases} \forall \text{i} = \overline{1, \text{z}} \qquad (3.41)$$

Збиток, нанесений *l*-м ФІП незахищеною ІП дорівнює:

$$u_l = \sum_{l=1}^{z} (\bar{h}_{li} * S_{\text{IP.i}}). \qquad (3.42)$$

Алгоритми визначення вартості інформаційних ресурсів. Найбільш складним питанням є оцінка вартості ІР. Нехай вони представлені у вигляді скінченної множини елементів і необхідно оцінити сумарну їх вартість в грошових одиницях.

Запропоновано наступний алгоритм оцінки вартості ІР.

1) Розділимо ІР на дві категорії:

- ресурси, вартість яких можна визначити, виходячи з витрат на їх придбання та обслуговування;
- ресурси, цінність яких є концептуальною, що не приносять безпосередньої прибутку, але втрата або псування яких завдасть підприємству збиток.

2) Вартість ресурсу з 1-ї категорії

$$S_{\text{IP.i}}^{1\text{кат}} = \frac{S_{\text{i}}^{\text{прид}}}{t_{\text{IP.i}}} + S_{\text{i}}^{\text{обсл}}, \text{i} = \overline{1, \text{z}_{1\text{кат}}}, \qquad (3.43)$$

де $S_{\text{i}}^{\text{прид}}$ - вартість придбаного ІР (якщо ресурс не придбаний, а створений в самій організації, то сюди входить сума витрат на його розробку), $t_{\text{ИР.i}}$ - термін експлуатації ресурсу в роках, $S_{\text{i}}^{\text{обсл}}$ - вартість обслуговування ІР за рік.

3) Оцінка вартості ресурсів 2-ї категорії починаємо з визначення цінності ІР і 1-й і 2-ї категорії на основі рангової шкали (по табл. 3.6).

Вектор цінності за оцінкою ε-го експерта:

$$C_{\varepsilon}=\{\ C_1^{\varepsilon},\ C_2^{\varepsilon},\ldots\ldots\ C_z^{\varepsilon}\}. \tag{3.44}$$

Для кожного і-го ресурсу j-м експертом визначено ранг C_{i}^{j}.

4) групуємо оцінки ресурсів 1-ї категорії так, щоб в кожній з максимум 9 груп (9 градацій в таблиці 3.6) були ресурси з однаковим значенням рангу.

Розглянемо групу зі значенням рангу R. Нехай вона складається з z_Rелементів. Обчислимо середню вартість ресурсу в даній групі:

$$E_R = \frac{1}{z_R}\sum_{\text{i}=1}^{z_R} S_{\text{IP.i}}^{\text{1кат}}\ . \tag{3.45}$$

Отриману величину можна вважати вартістю ресурсу, має ранг R. Ряд отриманих величин повинен бути впорядкований по зростанню, і повинна бути виконана умова суттєвої різниці оцінок при істотній відмінності рангів (відповідно до лінгвістичними описами табл. 3.6):

$$\begin{cases} E_R < E_{R+1,} & (\forall \text{R} = \overline{1,8} \\ E_{R_1} << E_{R_2}, & (R_2 \geq R_1 + 2) \end{cases}. \tag{3.46}$$

5) Якщо умова (3.46) не виконано, то експерт повинен скорегувати результати, отримані по (3.45) відповідно до (3.46).

6) Далі всім ІР з 2-ї категорії, які мають ранг R, присвоюємо значення вартості рівне E_R.

$$E_R \underset{C_{\text{i}}^{\varepsilon}=R}{\longrightarrow} S_{\text{ИР.i}}^{\text{2кат}}, \ (\forall \text{i} = \overline{1, \text{z}_{\text{2кат}}}). \tag{3.47}$$

7) Загальна вартість ІР за оцінками ε-го експерта визначаємо підсумовуванням:

$$S_{\text{IP}}^{\varepsilon} = \sum_{\text{i}=1}^{z_{\text{I}}} S_{\text{IP.i}}^{\varepsilon} \tag{3.48}$$

Вартість елементів ІП, схильних до впливу ФІП S_{OI}, визначатимемо підсумовуванням вартості всіх пристроїв в розрахунку на певний період:

$$\text{S}_{\text{OI}} = \sum_{k=1}^{z_{\text{OI}}} \frac{S_{\text{OI.k}}}{t_k} \tag{3.49}$$

де $S_{\text{OI.k}}$ - вартість елемента, t_k - термін служби пристрою (в роках). Вартість елементів СЗДІ $\text{S}_{\text{СОД}}$ також визначаємо в розрахунку на період шляхом підсумовування витрат на забезпечення достовірності по всіх позиціях [94], а також вартості технічних засобів забезпечення достовірності з урахуванням їх терміну служби:

$$\text{S}_{\text{СЗД}} = \sum_{k=1}^{z_{\text{заход}}} S_{\text{заход}.k} + \sum_{k=1}^{z_{TC}} \frac{S_{TC.k}}{t_k}. \tag{3.50}$$

Отже, порушення достовірності інформації несе в собі ризики для підприємств, організацій, чи, у випадку державних інформаційних ресурсів, для держави. Ризик для інформаційних ресурсів при відсутності систем забезпечення достовірності інформації являє собою функцію відносних частот виникнення факторів інформаційного протиборства та завданого збитку в разі порушення достовірності. Ступінь ризику залежить від вартості інформаційних ресурсів, що використовуються у процесах інформаційної взаємодії. Поділ інформаційних ресурсів на дві категорії вартості дає змогу, на основі експертного оцінювання, визначати найбільш доцільні заходи щодо забезпечення достовірності інформації, яка надається такими ресурсами кінцевим споживачам.

3.6. Узагальнення методики оцінки достовірності інформації в умовах інформаційного протиборства

Визначення ймовірності виникнення факторів інформаційного протиборства. Одним з методів формального визначення ймовірностей є статистична оцінка. Вона може бути адекватно застосована в тих випадках, коли є статистика для аналогічної ІП, експлуатованої з подібною специфікою діяльності, тобто коли можна говорити про наявність аналогічного набору СУ [90, 95]. Але в зв'язку з різноманіттям окремих характеристик ІП знайти аналог досліджуваної системи дуже непросто. Крім того, треба врахувати той факт, що отримати достовірну всеосяжну статистику по якомусь підприємству від нього буває дуже важко.

Коли така статистика недоступна, або в тому випадку, коли близьких аналогів досліджуваної ІП немає, адекватна оцінка відносних частот виникнення ФІП і можливостей збереження достовірності може бути

проведена тільки методами експертних оцінок на основі первинної оцінки не самих ймовірностей, а множини окремих показників, від яких вони залежать. Тоді деякий відсоток помилок в загальному масиві даних не на багато знизить адекватність експертизи.

Стан ІП характеризують не тільки можливості порушення достовірності інформації, а й відносні частоти виникнення факторів інформаційного протиборства (ФІП), що призводять до такого порушення.

Виникнення будь-якого ФІП навмисного дії обумовлено, з одного боку, наявністю в ІП СУ і, з іншого боку, зацікавленістю зловмисника у виконанні такої дії. Взаємодія двох систем: ІП підприємства та інформаційної системи зловмисника відбувається в єдиному інформаційному просторі. З точки зору забезпечення достовірності слід розглянути множину подій в цьому інформаційному просторі $E = \{ e_0 , e_1 ,..., e_n \}$, де подія e_0 полягає в тому, що в даний момент часу не виник ні один з повної множини ФІП, а події e_1, ..., e_n полягають у виникненні *l*-го ФІП, $l = \overline{1,n}$.

Множина $E = \{ e_0 , e_1 ,..., e_n \}$ є повною множиною незалежних і несумісних подій, тому що по-перше, виникнення одного ФІП не залежить від виникненням будь-якого іншого ФІП, по-друге, розглядається подія "виникнення *l*-го ФІП" відбувається в нескінченно малий проміжок часу і не може збігтися з іншою подією "виникнення *k*-го ФІП".

Імовірність виникнення ФІП залежить від зацікавленості зловмисника у виконанні несанкціонованих дій, природно, при наявності деякого СУ в ІП. Зацікавленість зловмисника у використанні СУ виразно залежить від того, наскільки значущий даний СУ для нормального функціонування ІП - чим більше значимість СУ, тим більше зацікавлений зловмисник в його використанні. Але на відносну частоту виникнення ФІП також впливає ще й обізнаність зловмисника про наявність СУ.

Відносну частоту виникнення ФІП $p_l^{\text{ФІП}}$ можна уявити як функцію значень критеріїв "значимість СУ" і "доступність СУ "для всіх СУ (тому що

один СУ може служити причиною появи декількох ФІП, і, навпаки, множина СУ може викликати появу одного ФІП):

$$p_l^{\text{ФІП}} = f\left(\gamma_{\alpha\beta}, d_\alpha, \forall\alpha, \beta = \overline{1, s}\right). \quad (3.51)$$

Для обчислення кількісного значення $p_l^{\text{ФІП}}$ необхідно:

- визначити повну скінченну множину СУ, характерних для даної ІП;
- отримати лінгвістичні експертні оцінки $\gamma_{\alpha\beta}, d_\alpha, \forall\alpha, \beta = \overline{1, s}$ від кожного ε-го експерта;
- визначити причинно-наслідкові зв'язки між *k*-м СУ і *l*-м ФІП;
- обчислити значення $p_{l\varepsilon}^{\text{ФІП}}$ за оцінками кожного ε-експерта;
- агрегувати отримані значення $p_{l\varepsilon}^{\text{ФІП}}$ тобто перетворити кожну нечітку множину $\text{A}(p_{\text{i}}^{\text{ФІП}}) = \text{A}\{p_{l\varepsilon}^{\text{ФІП}} / \varepsilon\}$ в чітке число $p_l^{\text{ФІП}}$.

На першому етапі даного алгоритму експертиза повинна бути проведена у вигляді круглого столу. Її результатом буде складання повного списку всіх СУ, характерних для даної ІП.

На другому етапі експерти представляють свої індивідуальні оцінки. Для коефіцієнтів значущості вони представлені у вигляді матриці парних порівнянь Сааті відповідно до табл. 3.2

$$\text{M}_\varepsilon^\Gamma = \begin{vmatrix} \gamma_{11}^\varepsilon & \gamma_{12}^\varepsilon & \cdots & \gamma_{1s}^\varepsilon \\ \gamma_{21}^\varepsilon & \gamma_{22}^\varepsilon & \cdots & \gamma_{2s}^\varepsilon \\ \cdots & \cdots & \cdots & \cdots \\ \gamma_{s1}^\varepsilon & \gamma_{s2}^\varepsilon & \cdots & \gamma_{ss}^\varepsilon \end{vmatrix} \quad (3.52)$$

Матриця (3.52) задовольняє висловом (3.17).

Оскільки кількість СУ типовий ІП обчислюється десятками, а то й сотнями, при чому їх завжди можна чітко розділити на групи, то для спрощення роботи по їх порівнянні раціонально використовувати метод перетворень по (3.22) - (3.27).

Вектор показників доступності визначаємо по табл. 3.3-3.5 як

$$D_{\varepsilon} = (d_1^{\varepsilon}, d_2^{\varepsilon} \ \dots \ , d_s^{\varepsilon}). \tag{3.53}$$

На третьому етапі перебування $p_l^{\text{ФІП}}$ необхідно побудувати матриці причинно-наслідкових зв'язків між *k*-м СУ і *l*-м ФІП

$$\mathrm{M}_{\varepsilon}^{\text{ПНЗ}} = \begin{vmatrix} \rho_{11}^{\varepsilon} & \rho_{12}^{\varepsilon} & \dots & \rho_{1s}^{\varepsilon} \\ \rho_{21}^{\varepsilon} & \rho_{22}^{\varepsilon} & \dots & \rho_{2s}^{\varepsilon} \\ \dots & \dots & \dots & \dots \\ \rho_{s1}^{\varepsilon} & \rho_{s2}^{\varepsilon} & \dots & \rho_{ss}^{\varepsilon} \end{vmatrix} \tag{3.54}$$

де p_{ik}^{ε}=1 вказує на те, що *k*-й СУ може бути причиною появи *l*-го ФІП на думку ε-го експерта, p_{ik}^{ε}= 0 - відповідно, не може.

Помноживши матрицю (3.54) розмірністю n×s на матрицю (3.52) розмірністю *s*×*s*, Отримаємо матрицю показників критичності СУ з розмірністю *n*×*s*

$$\mathrm{M}_{\varepsilon}^{\text{ПК}} = \mathrm{M}_{\varepsilon}^{\text{ПНЗ}} \times \mathrm{M}_{\varepsilon}^{\text{Г}} = \begin{vmatrix} \omega_{11}^{\varepsilon} & \omega_{12}^{\varepsilon} & \dots & \omega_{1s}^{\varepsilon} \\ \omega_{21}^{\varepsilon} & \omega_{22}^{\varepsilon} & \dots & \omega_{2s}^{\varepsilon} \\ \dots & \dots & \dots & \dots \\ \omega_{s1}^{\varepsilon} & \omega_{s2}^{\varepsilon} & \dots & \omega_{ss}^{\varepsilon} \end{vmatrix} \tag{3.55}$$

Величина $\omega_{ik}^{\varepsilon}$ показує ступінь впливу *k*-го СУ на появу *l*-го ФІП. Величини $\omega_{ik}^{\varepsilon}$ $\forall \mathrm{i} = \overline{1,\mathrm{n}},\ \mathrm{k} = \overline{1,\mathrm{s}}$ не нормовані, але при цьому максимальне значення такої величини показує максимальну ступінь впливу.

Нормалізація (приведення до шкали Сааті) повинна бути проведена з урахуванням діапазону значень в матриці (3.50) по

$$\begin{cases} \omega_{ik}^{\varepsilon} \to \omega_{ik}^{-\varepsilon} \\ max\ \gamma_{\alpha\,\beta}^{\varepsilon} \sim \max\omega_{ik}^{-\varepsilon}, \forall \mathrm{i} = \overline{1,\mathrm{n}}, \mathrm{k}, \alpha, \beta = \overline{1,\mathrm{s}} \\ min\ \gamma_{\alpha\,\beta}^{\varepsilon} \sim \min\omega_{ik}^{-\varepsilon} \end{cases} \tag{3.56}$$

Практична реалізація такого нормування може бути задана як

$$\bar{\omega}_{Ik}^{\varepsilon} = \left(\max_{\alpha,\beta=1,\ldots,s} \gamma_{\alpha\beta}^{\varepsilon} - \min_{\alpha,\beta=1,\ldots,s} \gamma_{\alpha\beta}^{\varepsilon} \right) \cdot \frac{\omega_{Ik}^{\varepsilon} - \min\limits_{\substack{I=1,\ldots,n \\ k=1,\ldots,s}} \omega_{Ik}^{\varepsilon}}{\max\limits_{\substack{I=1,\ldots,n \\ k=1,\ldots,s}} \omega_{Ik}^{\varepsilon} - \min\limits_{\substack{I=1,\ldots,n \\ k=1,\ldots,s}} \omega_{Ik}^{\varepsilon}} + \min_{\alpha,\beta=1,\ldots,s} \gamma_{\alpha\beta}^{\varepsilon} \tag{3.57}$$

Перетворення (3.57) призведе до того, що буде вірно

$$\begin{cases} \max\limits_{\substack{I=1,\ldots,n \\ k=1,\ldots,s}} \bar{\omega}_{Ik}^{\varepsilon} = \max\limits_{\alpha,\beta=1,\ldots,s} \gamma_{\alpha\beta}^{\varepsilon} \\ \min\limits_{\substack{I=1,\ldots,n \\ k=1,\ldots,s}} \bar{\omega}_{Ik}^{\varepsilon} = \min\limits_{\alpha,\beta=1,\ldots,s} \gamma_{\alpha\beta}^{\varepsilon} \end{cases} \tag{3.58}$$

при збереженні пропорцій між усіма значеннями з матриці (3.55).

Таким чином, отримаємо матрицю з нормованими значеннями

$$\bar{\mathrm{M}}_{\varepsilon}^{\mathrm{ПК}} = \begin{vmatrix} \bar{\omega}_{11}^{\varepsilon} & \bar{\omega}_{12}^{\varepsilon} & \ldots & \bar{\omega}_{1s}^{\varepsilon} \\ \bar{\omega}_{21}^{\varepsilon} & \bar{\omega}_{22}^{\varepsilon} & \ldots & \bar{\omega}_{2s}^{\varepsilon} \\ \ldots & \ldots & \ldots & \ldots \\ \bar{\omega}_{n1}^{\varepsilon} & \bar{\omega}_{n2}^{\varepsilon} & \ldots & \bar{\omega}_{ns}^{\varepsilon} \end{vmatrix} \tag{3.59}$$

Матрицю (3.59) необхідно доповнити вектором (3.53) і отримаємо

$$\mathrm{M}_{\varepsilon}^{\Phi\mathrm{IП}} = \begin{vmatrix} 10-d_1^{\varepsilon} & 10-d_2^{\varepsilon} & \dots & 10-d_s^{\varepsilon} \\ \bar{\omega}_{11}^{\varepsilon} & \bar{\omega}_{12}^{\varepsilon} & \dots & \bar{\omega}_{1s}^{\varepsilon} \\ \bar{\omega}_{21}^{\varepsilon} & \bar{\omega}_{22}^{\varepsilon} & \dots & \bar{\omega}_{2s}^{\varepsilon} \\ \dots & \dots & \dots & \dots \\ \bar{\omega}_{n1}^{\varepsilon} & \bar{\omega}_{n2}^{\varepsilon} & \dots & \bar{\omega}_{ns}^{\varepsilon} \end{vmatrix} \tag{3.60}$$

Нульовий рядок даної матриці показує вплив показника «доступність СУ» на виникнення в будь-який момент часу ситуації, коли немає ніяких ФІП.

Далі необхідно визначити сумарний показник впливу всіх СУ на виникнення l-го ФІП як

$$\omega_l^{\varepsilon} = \sum_{k=1}^{s} \omega_{lk}^{-\varepsilon}, \forall \mathrm{i} = \overline{0, \mathrm{n}}. \tag{3.61}$$

Виходячи з тверджень, наведених на початку розділу, розподіл сумарних показників впливу відповідає розподілу частот виникнення ФІП, яке можна отримати так:

$$p_{l\varepsilon}^{\Phi\mathrm{IП}} = \omega_l^{\varepsilon} \left(\sum_{l=0}^{n} \omega_l^{\varepsilon} \right)^{-1} \tag{3.62}$$

Агрегування отриманих значень $p_{l\varepsilon}^{\Phi\mathrm{IП}}$ з урахуванням коефіцієнтів авторитету експертів νε виробляємо наступним чином:

$$p_l^{\Phi\mathrm{IП}} = \frac{2*(m-2)!}{m!} \sum_{\alpha}^{m-1} \sum_{\beta=\alpha}^{m} \overline{H}_{\alpha\beta}, \tag{3.63}$$

де

$$H_{\alpha\beta} = \frac{v_{MAX}-v_{\alpha}}{v_{\alpha}-v_{\beta}}(p_{l\alpha}^{\text{ФІП}} - p_{l\beta}^{\text{ФІП}}) + p_{l\alpha}^{\text{ФІП}}, \bar{H}_{\alpha\beta} = \begin{cases} 0, & H_{\alpha\beta} < 0 \\ 0 \le H_{\alpha\beta} \le 1. \\ 1, & H_{\alpha\beta} > 1 \end{cases} \quad (3.64)$$

Агрегування по (3.63) і (3.64) можна застосувати до будь-якими параметрами, певним експертами і має бути використано для всіх експертних оцінок.

Збереження достовірності інформації. Можливості збереження достовірності *i*-го ІР під впливом *l*-го ФІП на думку ε-го експерта $p_{il\varepsilon}^{C}$ визначається тим, наскільки повно враховані якісні та кількісні вимоги до передачі, зберігання і обробці ІР:

$$p_{il\varepsilon}^{C} = f\left(x_{ilq_1}^{\Pi\varepsilon}, x_{ilq_2}^{X\varepsilon}, x_{ilq_3}^{O\varepsilon}, \forall \mathrm{q} \in \overline{1,\mathrm{t}}\right), \quad (3.65)$$

де $x_{ilq_1}^{\Pi\varepsilon}, x_{ilq_2}^{X\varepsilon}, x_{ilq_3}^{O\varepsilon}$ - ступеня виконання q-ї вимоги щодо функціонування відповідно механізмів передачі, зберігання або обробки *i*-го ІР в умовах впливу *l*-го ФІП.

Нехай перші h-вимоги будуть кількісними ($q=\overline{1,h}$) інші t-h – якісним ($q=\overline{h+1,t}$).

Ступінь виконання кількісного вимоги визначається його ставленням до необхідного (оптимального) кількісному значенню параметра СЗДІ. Процедури отримання оцінок кількісних параметрів розглянуті в п.3.3.

Для оцінки ступеня виконання якісних вимог (а таких вимог в різних стандартах незрівнянно більше, ніж кількісних) необхідно використовувати уявлення вимоги у вигляді нечіткої множини.

Ступінь виконання кожного якісного вимоги визначається функцією приналежності ряду характеристик СЗДІ, від яких залежить виконання цієї вимоги, до їх оптимальних значень.

Нехай $G=\{g_1, g_2,...,g_p\}$ – універсальна множина характеристик СЗДІ. На множині G задано нечітку множину A_q, яка відбиває ступінь приналежності СЗДІ до оптимальної по q-му вимогу.

Нечітка множина A_q, визначається :

1) Множиною ступенів відповідності кожної характеристики СЗДІ виконання q-го якісного вимоги $Y_q = \{y_1, y_2,...,y_p\}$.

2) Множиною ступенів впливу характеристик на виконання вимоги в цілому $\Sigma_q = \{\sigma_1, \sigma_2,...,\sigma_p\}$.

Якщо деяка характеристика повністю задовольняє вимогу, то її ступінь відповідності дорівнює 1, якщо повністю не задовольняє, то 0.

В цілому ступінь відповідності визначається відношенням до необхідного якісному опису характеристики СЗДІ, тобто функцією приналежності. Базовими відносинами для рівня відповідності реальної характеристики системи вимогу стандарту є: «низький», «нижче середнього», «середній», «вище середнього», «високий» [106]. На множині упорядкованих описів характеристики в порядку проходження від повного невідповідності до повної відповідності стандарту будуть відносини, представлені на рис. 3.8.

Приклад узятий для десяти можливих описів.

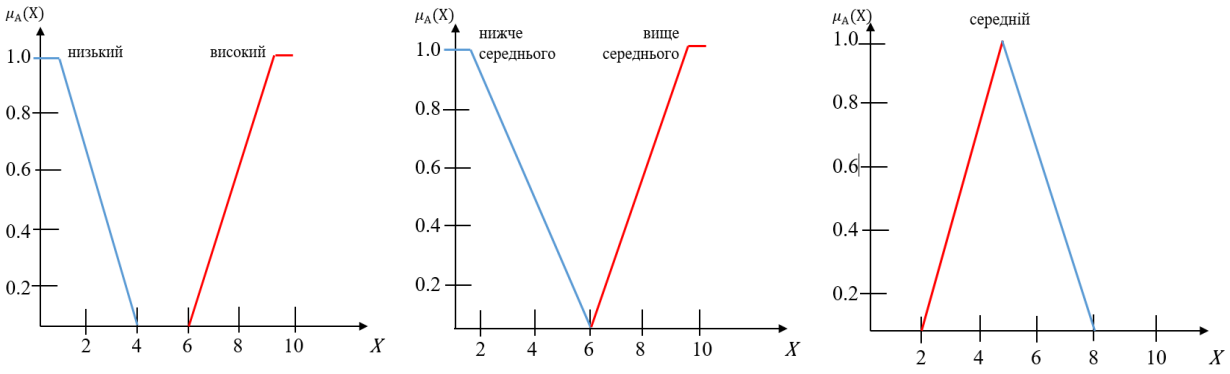

Рис. 3.8. Базові відносини рівня відповідності характеристики вимогу

Використовуючи такі операції над нечіткими множинами, як доповнення, перетин, об'єднання, концентрація і розмиття можна отримати функцію приналежності для будь-якого якісного експертного опису, побудованого на основі базових [122, 123]. Значення функції належності в точці X, відповідної досліджуваної характеристиці СЗДІ, буде шуканим числовим значенням.

Ступінь впливу характеристики СЗДІ на виконання вимоги можна знайти з матриці парних порівнянь

$$M_{\varepsilon}^{\Sigma} = \begin{vmatrix} \sigma_{11}^{\varepsilon} & \sigma_{12}^{\varepsilon} & \dots & \sigma_{1p}^{\varepsilon} \\ \sigma_{21}^{\varepsilon} & \sigma_{22}^{\varepsilon} & \dots & \sigma_{2p}^{\varepsilon} \\ \dots & \dots & \dots & \dots \\ \sigma_{p1}^{\varepsilon} & \sigma_{p2}^{\varepsilon} & \dots & \sigma_{pp}^{\varepsilon} \end{vmatrix} \qquad (3.66)$$

де $\sigma_{\alpha\beta}^{\varepsilon}$, $\forall \alpha,\beta=\overline{1,p}$ показує, наскільки вплив α –й характеристики істотніше впливу β –й.

Матриця (3.66) зазвичай має малу розмірність (кількість характеристик, від яких залежить вимога і складає одиниці для кожного вимоги.

Розподіл ступенів впливу характеристик задано власним вектором $\Sigma_{\varepsilon}=\{\sigma_{\alpha}^{\varepsilon}\}$ $\alpha=\overline{1,p}$, обчисленим для максимального власного числа матриці (3.66).

Ступінь виконання q-го якісного вимоги за оцінками ε-го експерта може бути знайдена за формулою

$$x_{ilq}^{\varepsilon} = \sum_{\alpha=1}^{p} y_{\alpha}^{\varepsilon}\, \sigma_{\alpha}^{\varepsilon}. \qquad (3.67)$$

При цьому ступінь виконання

$x_{ilq}^{\varepsilon}(\forall q = \overline{h+1,t},\ \forall i = \overline{1,z},\ \forall i = \overline{1,n},\ \forall \varepsilon = \overline{1,m,})$ задовольняють умові $0 \leq x_{ilq}^{\varepsilon} \leq 1$.

Можливість збереження достовірності *i*-го ІР під впливом *l*-го ФІП на думку *ε*-го експерта визначається як

$$p_{il\varepsilon}^{C} = \sum_{q_1}(v_{iq_1}^{\varepsilon} * x_{ilq_1}^{\varepsilon}) * \sum_{q_2}(v_{iq_2}^{\varepsilon} * x_{ilq_2}^{\varepsilon}) * \sum_{q_3}(v_{iq_3}^{\varepsilon} * x_{ilq_3}^{\varepsilon}), \qquad (3.68)$$

де $0 \leq v_{iq}^{\varepsilon} \leq 1$ - вагові коефіцієнти важливості вимог щодо протидії ФІП за оцінкою ε-го експерта за умови, що

$$\sum_{q=1}^{t} v_{iq}^{\varepsilon} = 1, (\forall i = \overline{1,z},\ \forall \varepsilon = \overline{1,m}). \qquad (3.69)$$

Звичайно, цей коефіцієнт, який визначає відносну значимість деякого умови, можна визначати за методами, викладеними в п. 3.4, але зазвичай кількість вимог обчислюється десятками-сотнями (кількість порівнянь відповідно - сотні-тисячі), а кількість ФІП - також десятками, то загальне число порівнянь виходить близько десятків тисяч; спрощений варіант порівнянь з поділом, скажімо, на десять груп дасть в десять разів менше дій, тобто декілька тисяч.

Викладене неможливо провести за прийнятний час. Та й кількість операцій в кілька тисяч, звичайно, не в сотню разів підвищить адекватність оцінки в порівнянні з кількістю в кілька десятків.

Запропоновано наступний алгоритм проведення оцінки. Експерт заповнює попередню матрицю

$$\mathrm{M}_{\varepsilon}^{V^I} = \begin{vmatrix} v_{11}^{I^\varepsilon} & v_{12}^{I^\varepsilon} & \dots & v_{1t}^{I^\varepsilon} \\ v_{21}^{I^\varepsilon} & v_{22}^{I^\varepsilon} & \dots & v_{2t}^{I^\varepsilon} \\ \dots & \dots & \dots & \dots \\ v_{n1}^{I^\varepsilon} & v_{n2}^{I^\varepsilon} & \dots & v_{nt}^{I^\varepsilon} \end{vmatrix} \quad (3.70)$$

де $v_{iq}^{I^\varepsilon}, (\forall \mathrm{q} = \overline{1,\mathrm{t}}, \forall \mathrm{i} = \overline{1,\mathrm{n}}, \forall \varepsilon = \overline{1,\mathrm{m}})$ показує окрема вплив q-го вимоги для усунення і-го ФІП за оцінкою ε-го експерта. ця величина може бути задана в межах шкали балів (0 .. 5) по табл. 3.7.

Далі можливо перетворення виду

$$v_{\mathrm{iq}}^{\varepsilon} = \frac{v_{iq}^{I^\varepsilon}}{\sum_{q=1}^{t} v_{iq}^{I^\varepsilon}} (\forall \mathrm{i} = \overline{1,\mathrm{n}}, \forall \varepsilon = \overline{1,\mathrm{m}}), \quad (3.71)$$

що задовольняє умові (3.69).

Таким чином, отримуємо матрицю

$$\mathrm{M}_{\varepsilon}^{V} = \begin{vmatrix} v_{11}^{\varepsilon} & v_{12}^{\varepsilon} & \dots & v_{1t}^{\varepsilon} \\ v_{21}^{\varepsilon} & v_{22}^{\varepsilon} & \dots & v_{2t}^{\varepsilon} \\ \dots & \dots & \dots & \dots \\ v_{t1}^{\varepsilon} & v_{t2}^{\varepsilon} & \dots & v_{tt}^{\varepsilon} \end{vmatrix} \quad (3.72)$$

Таблиця 3.7

Шкала оцінки впливу вимог на збереження достовірності [90]

Опис виду впливу	Бал
Абсолютна і постійний вплив в будь-яких умовах	5
Впливає практично у всіх умовах	3
Впливає тільки в окремих випадках (наприклад, при використані зловмисником спецзасобів)	1
Не впливає	0

Значення 2 і 4 можуть бути взяті як проміжні.

Оцінка загального показника достовірності інформації. З (2.1) з використанням (3.63) і (3.68) знаходимо окремі показники достовірності окремих ІР. Оскільки різні ресурси надають різний вплив на якість функціонування ІП, то необхідно ввести деяку величину η_i^{ε} - ($\forall i=\overline{1, z_И}$), що показує відносну цінність і-го інформаційного ресурсу. Для комерційних підприємств цінність ресурсу завжди зводиться до його грошового еквівалента, отже, вона може бути визначена з (3.48) як

$$\eta_{\varepsilon_i} = \frac{S_{\varepsilon_{IP,i}}}{S_{\varepsilon_{IP}}}, (\forall i=\overline{1, z_I}). \quad (3.73)$$

Тоді загальний показник достовірності достовірність інформації в ІП за оцінкою ε-го експерта визначимо наступним чином:

$$D_\varepsilon = \sum_{i=1}^{z_I} \frac{S_{\varepsilon_{IP,i}}}{S_{\varepsilon_{IP}}} * D_{\varepsilon_i} \quad (3.74)$$

Таким чином, у разі відсутності статистики адекватна оцінка відносних частот виникнення факторів інформаційного протиборства та можливостей збереження достовірності інформації може бути проведена методами експертних оцінок на основі первинної оцінки множини початкових показників. У загальному випадку імовірність виникнення фактора інформаційного протиборства залежить від зацікавленості зловмисника у виконанні несанкціонованих дій при наявності деяких уразливостей в інформаційному просторі організації. На основі експертного оцінювання кількісних та якісних вимог, у тому числі з нечіткими змінними, досягається можливість оцінки загального показника достовірності інформації у вигляді

комбінації окремих показників достовірності окремих інформаційних ресурсів.

Висновки до розділу 3

1. Методика оцінки поточного рівня достовірності інформації як ймовірності збереження її незмінності в інформаційному потоці в умовах інформаційних впливів вимагає врахування: частоти виникнення факторів інформаційного протиборства, можливості порушення достовірності, ймовірності виявлення спроб порушення достовірності інформації. Інформаційний простір організації, підприємства, держави дуже часто складається з множини різнорідних компонентів, що не дає можливості одержувати числові компоненти статистичними методами. Відтак, найбільш доцільними тут є методи експертного оцінювання.

2. Через необхідність регулярної оцінки поточного рівня достовірності при значній кількості елементів інформаційного простору основною процедурою оцінювання є однотурова анонімна процедура на основі математичних методів згладжування неузгодженостей оцінок експертів. Оцінку кількісних параметрів найбільш доцільно реалізувати в шкалах у відповідності з фізичним змістом параметра. Отримані якісні оцінки перетворюються у кількісні значення за таблицями відповідності або з використанням баз знань, після чого оцінюються як кількісні параметри.

3. Чіткі кількісні параметри оцінюються або в абсолютних величинах, або в нормованих відповідно до обраної шкали нормування. У якості шкал використовуються шкала інтервалів, шкала відносин, шкала різниць або абсолютна шкала. Нечіткі кількісні параметри оцінюються, як правило, за

нечітким числом з трикутною (симетричною чи несиметричною) функцією приналежності. При цьому експерти представляють свої оцінки у вигляді трійки чисел. За необхідності, точність оцінювання може бути підвищена шляхом використання уточнюючого коефіцієнта авторитету.

4. Для оцінки якісних параметрів необхідно спочатку розділити їх на ті, які мають точний опис, тобто існує або може бути задана послідовність описів, упорядкованих за ранговою шкалою. Такі параметри можуть бути оцінені шляхом використання прямого перетворення по лінгвістичним таблицям або за допомогою парних порівнянь альтернатив. Оцінка якісних параметрів передбачає на першому етапі оцінку значимості умов, зокрема структурно-функціональних недоліків інформаційної взаємодії. На другому етапі здійснюється лінгвістичний опис варіантів оцінки елемента і присвоєння їм числових значень. Одержані оцінки заносяться у матрицю часткових оцінок, яка для декількох груп експертів буде мати блочний вигляд. Порівняння альтернатив здійснюється за сумою рангів рядків матриці за відповідними групами. Перевагою такого підходу є значне зниження кількості порівнянь. Крім того, запропонований підхід дозволяє враховувати авторитетність окремого експерта та неузгодженість думок експертів під час оцінювання.

5. Порушення достовірності інформації несе в собі ризики для підприємств, організацій, чи, у випадку державних інформаційних ресурсів, для держави. Ризик для інформаційних ресурсів при відсутності систем забезпечення достовірності інформації являє собою функцію відносних частот виникнення факторів інформаційного протиборства та завданого збитку в разі порушення достовірності. Ступінь ризику залежить від вартості інформаційних ресурсів, що використовуються у процесах інформаційної взаємодії. Поділ інформаційних ресурсів на дві категорії вартості дає змогу, на основі експертного оцінювання, визначати найбільш доцільні заходи щодо забезпечення достовірності інформації, яка надається такими ресурсами кінцевим споживачам.

6. У разі відсутності статистики адекватна оцінка відносних частот виникнення факторів інформаційного протиборства та можливостей збереження достовірності інформації може бути проведена методами експертних оцінок на основі первинної оцінки множини початкових показників. У загальному випадку імовірність виникнення фактора інфомаційного протиборства залежить від зацікавленості зловмисника у виконанні несанкціонованих дій при наявності деяких уразливостей в інформаційному просторі організації. На основі експертного оцінювання кількісних та якісних вимог, у тому числі з нечіткими змінними, досягається можливість оцінки загального показника достовірності інформації у вигляді комбінації окремих показників достовірності окремих інформаційних ресурсів.

РОЗДІЛ 4.
ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ МЕТОДИКИ ОЦІНКИ ДОСТОВІРНОСТІ ІНФОРМАЦІЇ В УМОВАХ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЇЇ ЗАСТОСУВАННЯ

4.1. Формування початкових даних для оцінка показників достовірності інформації в умовах інформаційного протиборства

Для перевірки істинності одержаних наукових результатів та загальної ефективності методики оцінки достовірності інформації було проведено моделювання процесів забезпечення достовірності на прикладі типової компанії. На рис. 4.1. зображено типову організаційну структуру компанії.

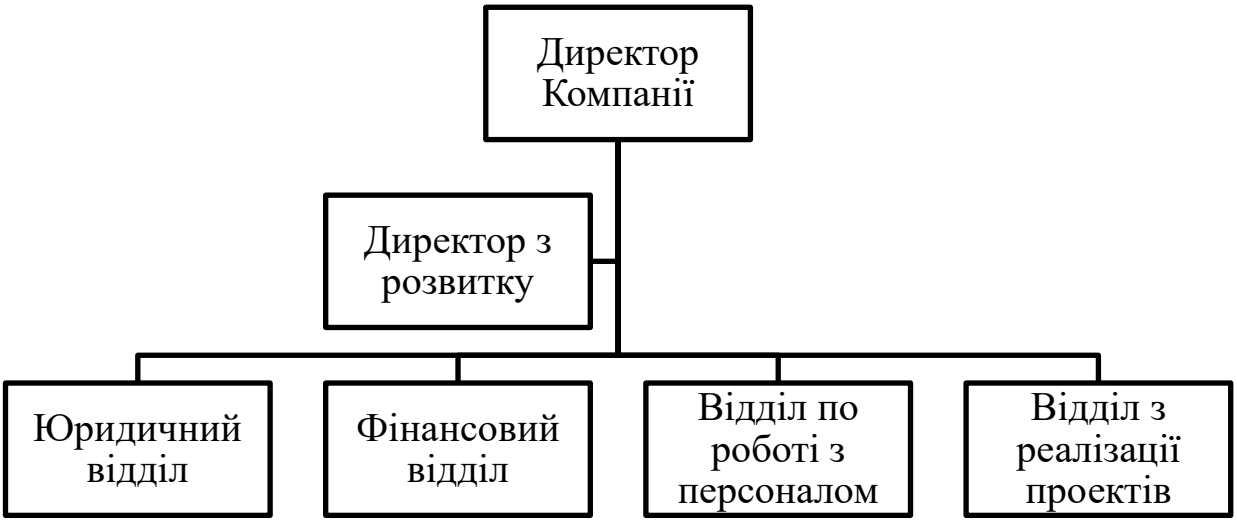

Рис. 4.1. Типова організаційна структура Компанії

До інформаційних ресурсів відносимо:

1. Інформація органів державної влади;
2. Укази Президента;
3. Заяви високопосадовців;
4. Виступи на конференціях високопосадовців;
5. Повідомлення на офіційних веб-порталах органів державної влади;
6. Статті на веб-порталах інформаційних агенств;
7. Оголошення державного радіомовника;
8. Огляди блогерів;
9. Блоки соціальної реклами;
10. Пости в соціальних мережах на суспільно-політичну тематику.

До джерел інформаційних ресурсів відносимо:

1. Органи державної влади;
2. Офіційний веб-портал органу державної влади;
3. Блоги;
4. Соціальні мережі (сторінки користувачів, групи, тематичні сторінки);
5. Телебачення;
6. Інтернет-видання;
7. Радіо;
8. Друковані ЗМІ;
9. Статистична інформація;
10. Соціологічні дослідження.

Елементи та засоби обробки та передачі інформації:

1. Особисте спілкування;
2. Телефонні розмови;

3. Електронні листи;
4. Соціальні мережі;
5. Месенджери;
6. Телебачення;
7. Радіо;
8. Друковані видання;
9. Реклама;
10. Блоги.

Множина каналів інформаційного впливу (КІВ):

1. Особисте спілкування;
2. Телефонні розмови;
3. Електронні листи;
4. Чати в соціальних мережах;
5. Повідомлення з месенджерів;
6. Телебачення;
7. Радіо;
8. Друковані видання;
9. Відеохостинги;
10. Блоги.

Множина факторів інформаційного протиборства (ДФ – загрози достовірності):

1. Маніпулювання достовірною інформацією.
2. Тенденційний підбір тем та матеріалів.
3. Відволікання уваги прихильників від дійсно значимого, але політично невигідного для представлення події, неякісним представленням інформаційного матеріалу.
4. Вибір вигідного моменту для інформування населення.

5. Емоційне коментування, представлення подій.

6. Використання думок компетентних осіб, які поважаються суспільством.

7. Визначена послідовність представлення інформації: при оголошенні суперечливих точок зору, найбільш переконливою вважається та інформація, яка представлена першою.

8. Демонстрація в пропагандистських матеріалах переваг своєї культури (цивілізації).

9. Використання ЗМІ як інструменту безпосереднього доведення до суспільства і окремих особистостей загроз, ультиматумів, "імпульсів" диктату і залякування.

10. Використання ЗМІ як каналу доведення населення, керівництва держави націленої дезінформації.

Засоби системи забезпечення достовірності інформації (СЗДІ):

1. Нейтралізація негативних інформаційних впливів.

2. Адаптація особистості (соціальної організації) до інформаційних впливів.

3. Зміцнення корпоративної культури, тобто діяльність адміністрації по створенню такого морально-психологічного клімату, який би сприяв з мінімальним збитком протидіяти інформаційним впливам та успішно виконувати виробничі та інші завдання.

4. Робота по ліквідації (послабленню) інформаційних вторгнень;

5. Інформування співробітників про проведені заходи з інформаційної безпеки.

6. Проведення лекцій щодо інформаційної гігієни.

7. Попередження співробітників про можливі фішингові атаки.

8. Унеможливлення маніпулятивних впливів на інформацію, яка подається керівництвом.

9. Фільтрація інформації, що надходить з недовірених джерел інформації.

10. Звернення до першоджерела.

Для проведення дослідження було сформовано групу експертів, з числа науково-педагогічних працівників Навчально-наукового інституту захисту інформації Державного університету телекомунікацій.

У якості експертів виступили:

1. Савченко В.А. – д.т.н., професор, директор Навчально-наукового інституту захисту інформації.

2. Гайдур Г.І. – д.т.н., професор, завідувач кафедри Інформаційної та кібернетичної безпеки.

3. Легомінова С.В. – д.е.н., професор, завідувач кафедри Управління інформаційною та кібернетичною безпекою.

4. Довженко Н.М. – к.т.н., доцент, доцент кафедри Інформаційної та кібернетичної безпеки.

5. Дзюба Т.М. – к.т.н., доцент, доцент кафедри Управління інформаційною та кібернетичною безпекою.

Зазначені експерти встановили початкові значення важливості каналів інформаційного впливу (табл. 4.1), ступінь доступності каналів інформаційного впливу (табл. 4.2), ступінь впливу факторів інформаційного протиборства на інформаційні ресурси (табл. 4.3) та ступінь відповідності характеристик системи забезпечення достовірності інформації висунутим вимогам (табл. 4.4).

Таблиця 4.1

Порівняння значень важливості каналів інформаційного впливу

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	1	8	7	6	1/5	1/6	1/7	1	1	1
2	1/8	1	1/7	1/5	1/9	1/9	1/9	1	1/6	1/9
3	1/7	7	1	3	1/7	1/7	1/7	1	1/5	1/8

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
4	1/6	5	1/3	1	1/9	1/9	1/9	1	1/5	1/7
5	5	9	7	9	1	1/7	1/7	1	1/7	1/6
6	6	9	7	9	7	1	1	1	1/7	1/5
7	7	9	7	9	7	1	1	1	1/9	1/4
8	1	1	1	1	1	1	1	1	1	1
9	1	9	7	7	5	5	6	1	1	1
10	1	9	8	7	6	5	4	1	1	1

Таблиця 4.2

Вектор доступності каналів інформаційного впливу

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
0,3	0,1	0,7	0,5	0,5	0,3	0,3	0,5	0,5	0,9

Таблиця 4.3

Матриця оцінки ступеня впливу факторів інформаційного протиборства на інформаційні ресурси

		Інформаційні ресурси									
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Фактори інформаційного протиборства	1	0,07	0,07	0,05	0,06	0,06	0,05	0,07	0	0	0
	2	0,02	0,02	0,07	0,02	0,02	0,07	0,02	0,08	0,07	0,04
	3	0,07	0,07	0,05	0,06	0,06	0,05	0,07	0	0	0
	4	0,05	0,05	0,12	0,16	0,04	0,12	0,07	0,15	0,13	0,27
	5	0,02	0,02	0,02	0,02	0,02	0,02	0,02	0	0	0
	6	0,02	0,02	0,02	0,02	0,02	0,02	0,02	0,08	0,07	0,04
	7	0,05	0,05	0,03	0,04	0,04	0,03	0,05	0,15	0,13	0,08
	8	0,07	0,07	0,05	0,06	0,06	0,05	0,07	0	0	0
	9	0,1	0,1	0,07	0,08	0,09	0,07	0,09	0	0	0
	10	0,05	0,05	0	0	0	0	0	0	0	0

Таблиця 4.4

Оцінка ступеня відповідності характеристик СЗДІ висунутим вимогам

	Характеристики										
Вимоги		**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
	1			0,1	0,1		0,2	0,3		0,1	0,2
	2	0,8	0,1	0,1							
	3	0,8	0,6	0,1					0,8		

	Характеристики									
	4	0,1		0,1		0,3				0,5	
	5	0,8	0,6				0,1	0,2	0,2		
	6	0,3	0,3	0,1	0,2						
	7	1	0,8			0,3			0,2		
	8	0,8	0,8	0,1	0,1					0,2	
	9	0,8	0,5	0,1	0,1		0,2	0,3			0,3
	10	1	1			0,1					

Також, експертами було визначено вартість інформаційних ресурсів організації в розрахунку на 1 рік (табл. 4.5).

У якості основних інформаційних ресурсів аналізувалися:

1. Пости в соціальних мережах на суспільно-політичну тематику;
2. Огляди блогерів;
3. Повідомлення в місцевих ЗМІ.
4. Статті на веб-порталах інформаційних агентств.
5. Новини державних інформаційних агентств.
6. Оголошення державного телерадіомовника;
7. Виступи високопосадовців на прес-конференціях;
8. Офіційні заяви високопосадовців.
9. Інформація органів державної влади на офіційних веб-порталах.
10. Укази Президента України, Закони (рішення) Верховної ради України, постанови Кабінету міністрів України.

Для оцінки вартості ресурсів аналізувалися показники прибутковості організації у випадку своєчасного та повного використання інформації з відповідного ресурсу (табл. 4.5).

Таблиця 4.5

Вартість всіх інформаційних ресурсів в розрахунку на 1 рік

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
9400	9400	10600	11300	24600	28300	28300	37800	37800	37800

Сумарна вартість: 235 300 грн.

4.2. Результати розрахунку показників достовірності інформації в умовах інформаційного протиборства

На підставі порівняння значень важливості каналів інформаційного впливу, рейтингу джерел інформації у списках достовірних/недостовірних джерел експертами встановлено розподіл частот виникнення факторів інформаційного протиборства (табл. 4.6).

Таблиця 4.6

Розподіл частот виникнення факторів інформаційного протиборства

1	2	3	4	5	6	7	8	9	10
0,11	0,06	0,12	0,15	0,07	0,06	0,15	0,07	0,07	0,14

На підставі оцінки вартості інформаційних ресурсів (табл. 4.5), матриці оцінки ступеня впливу факторів інформаційного протиборства на інформаційні ресурси (табл. 4.3) визначено збиток, який може бути нанесено підприємству у результаті впливу факторів інформаційного протиборства (табл. 4.7).

Таблиця 4.7

Розподіл збитку, що нанесений фактором інформаційного протиборства

1	2	3	4	5	6	7	8	9	10
11130	6071	12141	40942	2306	4659	22942	7083	9883	3294

Таблиця 4.9

Ймовірність збереження достовірності інформації під дією факторів інформаційного протиборства

1	2	3	4	5	6	7	8	9	10
0,23	0,23	0,25	0,3	0,33	0,38	0,38	0,39	0,51	0,57

Шляхом експертного оцінювання було визначено достовірність окремих інформаційних ресурсів (рис. 4.1). У подальшому, графіки, що відображають

зміни достовірності інформаційних ресурсів, будуть побудовані у порядку збільшення їх значимості.

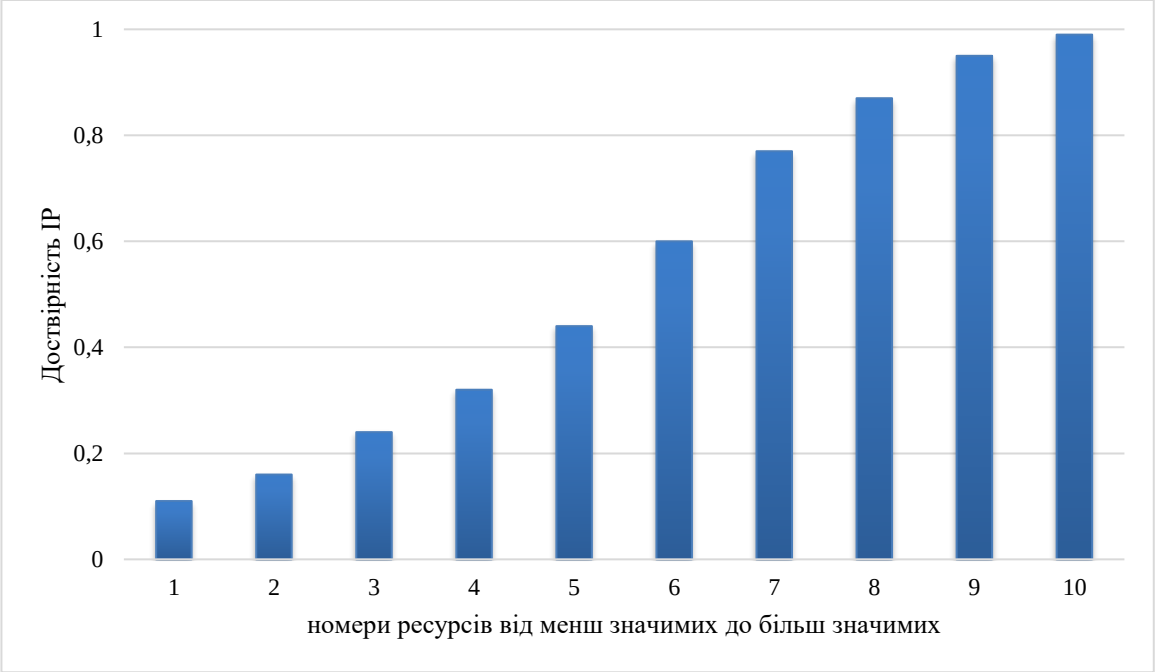

Рис. 4.1. Показники достовірності інформаційних ресурсів

Таким чином, достовірність інформаційного ресурсу є прямо залежною від його значимості.

Дослідження початкової достовірності інформації для організації в умовах інформаційного протиборства з урахування вичерпного списку інформаційних ресурсів, факторів протиборства та каналів впливу виявило наступні проблеми в забезпеченні достовірності інформаційних ресурсів організації:

– показники достовірності половини ресурсів нижче рівня 0,5, що в контексті нечітких оцінок відповідає опису «недостовірно»;

– найбільш цінні інформаційні ресурси захищені від дії факторів інформаційного протиборства відносно добре (достовірність більше 0,5), разом з тим, рівень достовірності локальних ресурсів та соціальних мереж є достатньо низьким.

Рішення по забезпеченню потрібного рівня достовірності. Для покращення ситуації з достовірністю інформаційних ресурсів було проведено заходи організаційного та технічного характеру, які можна поділити на 4 категорії:

1. Підвищення адекватності моделей представлених даних.
2. Підвищення якості організації інформаційного обміну.
3. Підвищення якості контролю інформаційного ресурсу.
4. Підвищення кваліфікації персоналу.

Результати повторного оцінювання достовірності наведено на рис. 4.2 – 4.5.

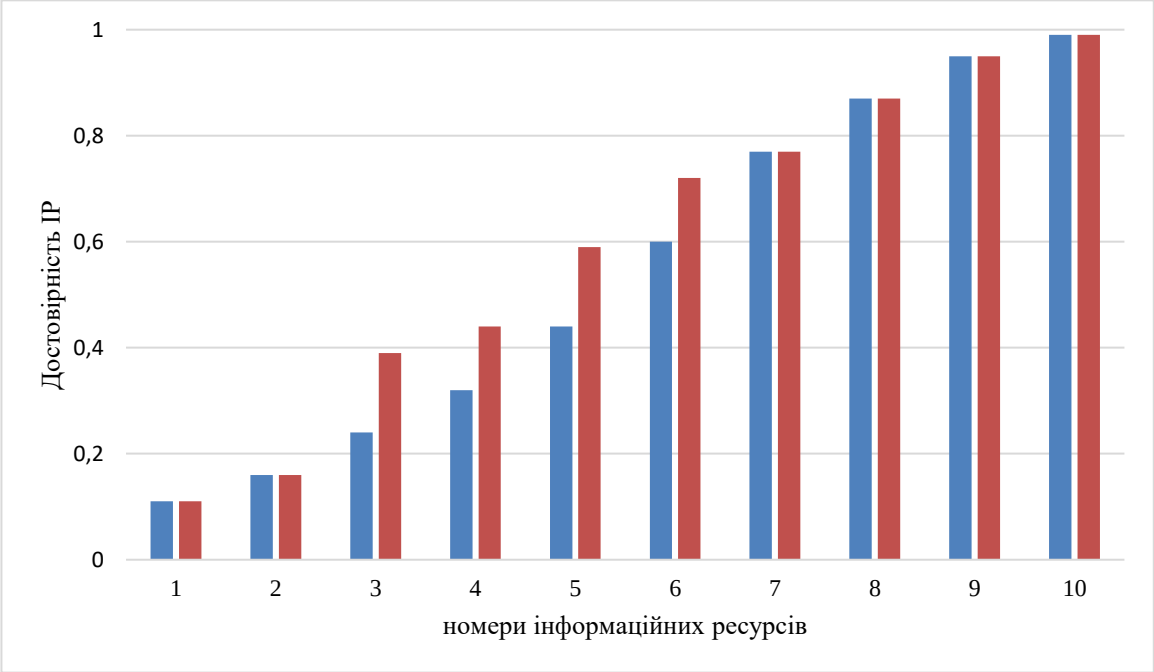

Рис. 4.2. Зміна показників достовірності при підвищенні адекватності моделей представлених даних

Як видно з рис. 4.2 підвищення адекватності моделей подання даних суттєво підвищує достовірність інформації у повідомленнях в місцевих ЗМІ, у статтях на веб-порталах інформаційних агентств, у новинах державних інформаційних агентств та оголошеннях державного телерадіомовника. При цьому загальний приріст достовірності становить 9–11%.

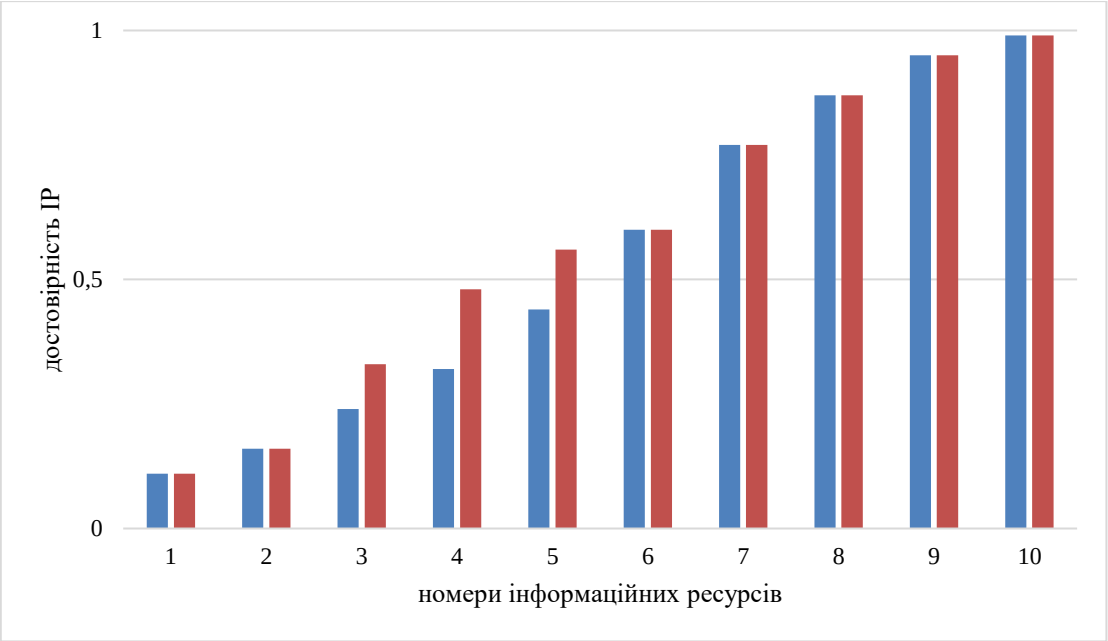

Рис. 4.3. Зміна показників достовірності при підвищенні якості організації інформаційного обміну

Якість організації інформаційного обміну (рис. 4.3) підвищує достовірність повідомлень, що передаються в місцевих ЗМІ, на веб-порталах інформаційних агенств та у новинах державних інформаційних агенств. При цьому загальний приріст достовірності становить 6–8%.

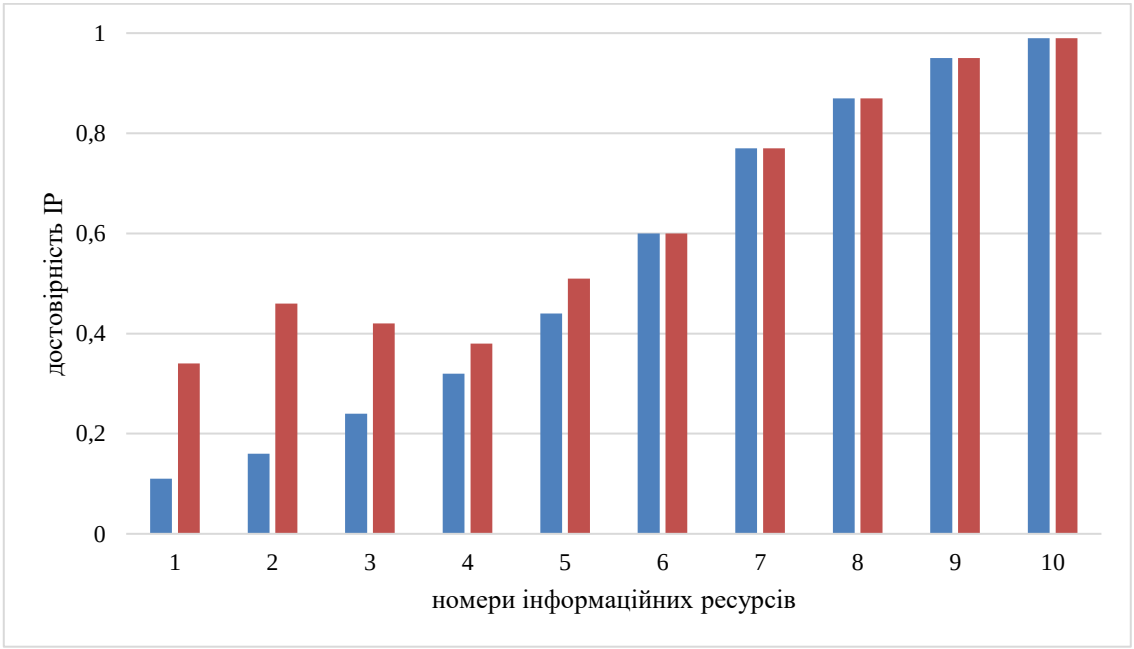

Рис. 4.4. Зміна достовірності IP при підвищенні якості контролю IP

Підвищення якості контролю інформаційних ресурсів (рис. 4.4) суттєво підвищує достовірність інформації, яка надходить з постів в соціальних мережах, оглядів блогерів, повідомлень в місцевих ЗМІ. При цьому загальний приріст достовірності становить 15–17%.

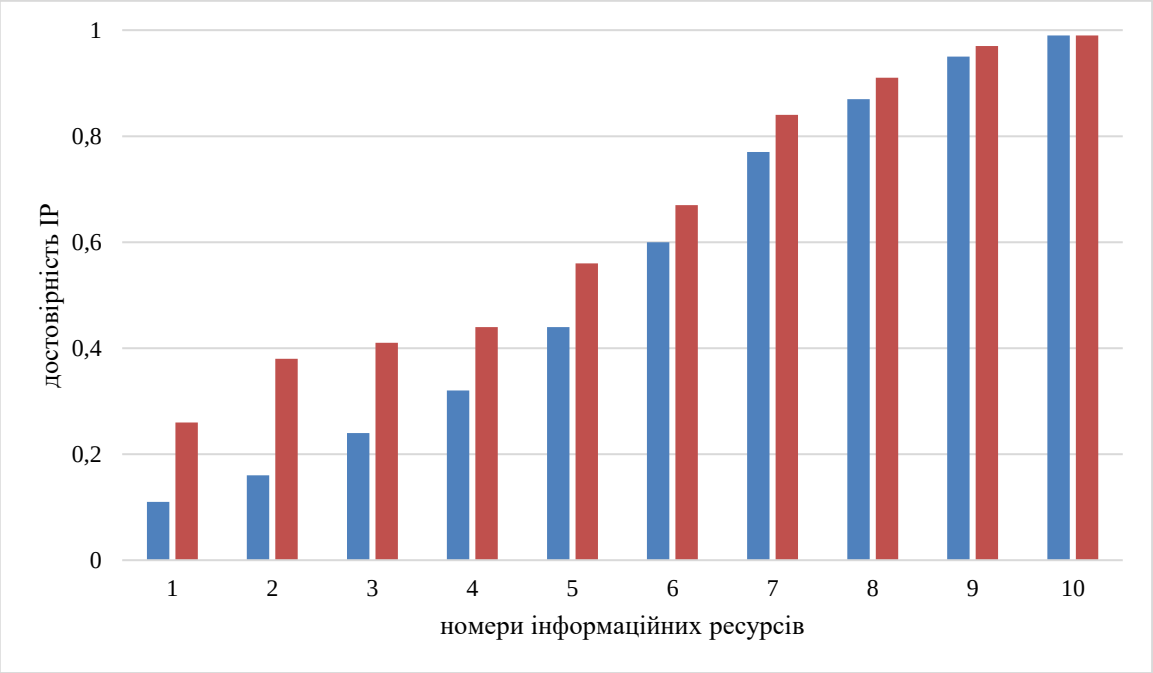

Рис. 4.5. Зміна достовірності IP при підвищенні кваліфікації персоналу

Підвищення кваліфікації персоналу (рис. 4.5) дає приріст практично по всім інформаційним ресурсам, оскільки у такому випадку персонал самостійно здатен аналізувати повідомлення на предмет достовірності. При цьому загальний приріст достовірності становить 17–19%.

Дослідження варіантів застосування системи забезпечення достовірності інформації. Попередній розгляд типової організації проводився без урахування заходів щодо підвищення її достовірності. Далі представлені результати перерахунку показників, які були отримані при реалізації заходів покращення достовірності (табл. 4.10 – 4.14).

Таблиця 4.10

Переоцінка ступеня відповідності характеристик СЗДІ пропонованим вимогам

	Характеристики										
Вимоги		1	2	3	4	5	6	7	8	9	10
	1			0,1	0,4		0,2	0,3		0,1	0,2
	2	0,8	0,1	0,1							
	3	0,8	0,6	0,1					0,8		
	4	0,1		0,1		0,3				0,5	
	5	0,8	0,6				0,1	0,2	0,5		
	6	0,3	0,3	0,1	0,2						
	7	1	0,8			0,5			0,2		
	8	0,8	0,8	0,1	0,4					0,2	
	9	0,8	0,5	0,4	0,1		0,5	0,3			0,3
	10	1	1			0,1					

Таблиця 4.11

Новий розподіл збитку, що нанесений ФІП

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
9106	4047	10118	30024	1647	4659	19883	6071	8471	3294

Таблиця 4.12

Нові ймовірності збереження достовірності інформації під дією ФІП

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
0,39	0,38	0,31	0,42	0,39	0,58	0,57	0,71	0,23	0,73

Таблиця 4.13

Достовірність окремих ІР, ранжованих по значимості

Заходи підвищення достовірності	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Початковий варіант	0,11	0,16	0,24	0,32	0,44	0,6	0,77	0,87	0,95	0,99
Підвищення адекватності моделей	0,11	0,16	0,39	0,44	0,59	0,72	0,77	0,87	0,95	0,99

Заходи підвищення достовірності	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Покращення інформаційного обміну	0,11	0,16	0,33	0,48	0,56	0,6	0,77	0,87	0,95	0,99
Покращення контролю інформаційних ресурсів	0,34	0,46	0,42	0,38	0,51	0,6	0,77	0,87	0,95	0,99
Підвищення кваліфікації персоналу	0,26	0,38	0,41	0,44	0,56	0,67	0,84	0,91	0,97	0,99

На рис. 4.6 представлені діаграми зміни показників достовірності для вище наведених варіантів покращення достовірності. Всі три варіанти не виходять за рамки економічної доцільності. Але тільки третій варіант забезпечує і найбільший спільний показник достовірності (0,84), і значення приватних показників всіх IP більше мінімально встановленої межі в 0,5.

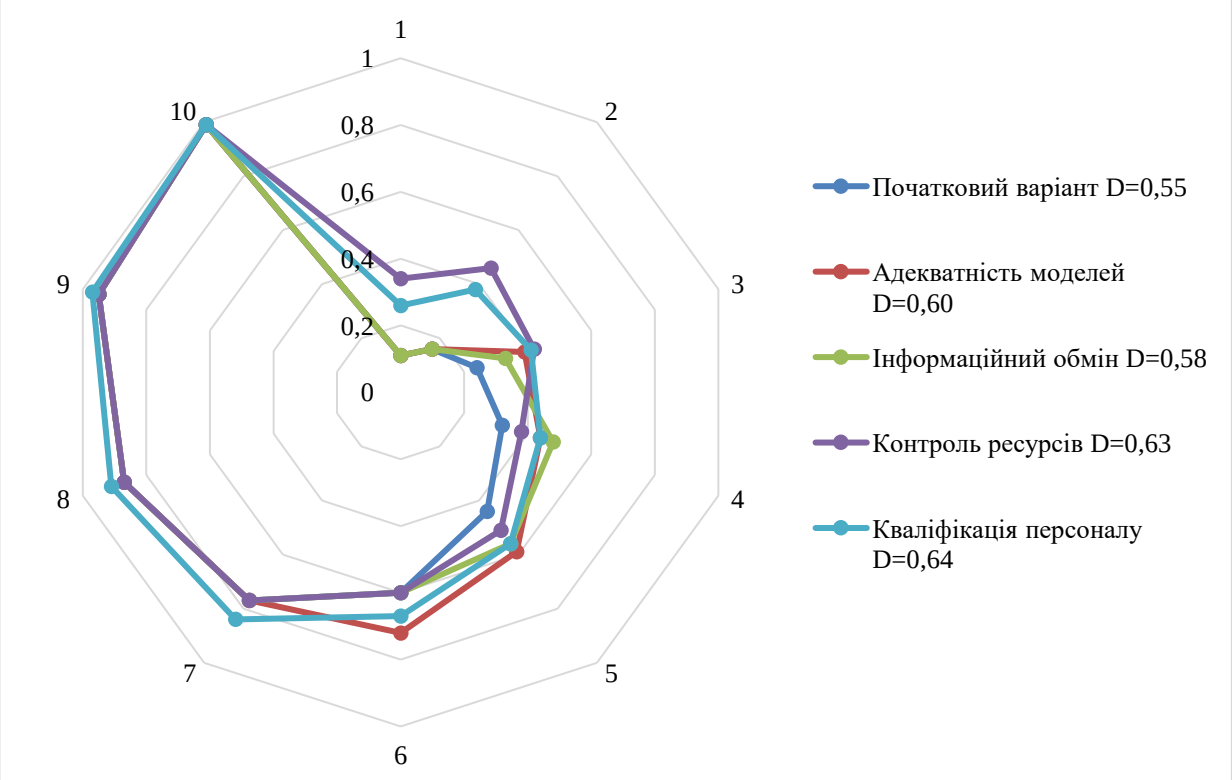

Рис. 4.6. Зміна показників достовірності IP

4.3. Розробка рекомендацій щодо забезпечення достовірності інформації в інформаційному просторі організації

Перевірка достовірності інформації є одним з необхідних елементів процесу прийняття рішень в будь-якій організації. Перевірка достовірності спрямована на виявлення невідповідності між наявними фактами та реальною дійсністю. Таку перевірку можна проводити як до прийняття рішення, так і після прийняття рішення. Перевірку достовірності інформації, як правило, проводять штатні посадові особи організації за напрямом діяльності. Разом з тим, деякі організації призначають для цього спеціальних осіб, завданням яких є робота щодо інформаційної підтримки рішень, у тому числі і здійснення контролю достовірності інформації. Таким чином, на теперішній час перевірка достовірності інформації є необхідним елементом будь-якого процесу прийняття рішень.

У той же час, у ході дослідження виявлено можливості щодо підвищення достовірності інформації, яка використовується для прийняття управлінських рішень. Зазначені заходи можуть бути проведені за трьома основними напрямами:

1. Побудова системи забезпечення достовірності інформації в організації. Зазначену систему можна спроектувати у двох варіантах: а) окремий підрозділ або посадова особа в організації (CIO – Chief Information Officer); б) розподіл обов'язків щодо контролю достовірності інформації між різними посадовими особами за напрямами діяльності: відділ кадрів працює з достовірністю HR, бухгалтерія – з економічною інформацією і т.д.

2. Раціональна організація процесу оцінки достовірності. Цей напрям охоплює процедури вибору експертів, порядку прийняття рішень, алгоритми перевірки як самої інформації, так і джерел інформації.

3. Технічне забезпечення контролю достовірності. У цьому напрямі розглядаються питання застосування програмних та апаратних комплексів контролю достовірності, оцінювання ризиків та технології протидії негативному впливові факторів інформаційного протиборства.

Рекомендації щодо побудови системи забезпечення достовірності інформації. Для великої організації чи корпорації найбільш доцільним буде реалізація варіанту з формуванням окремого підрозділу (структури), яка здійснюватиме оцінювання достовірності інформації для керівника. Часто такі функції покладаються на інформаційні чи інформаційно-аналітичні підрозділи організації. Організації меншого масштабу можуть призначати окрему посадову особу, в обов'язки якої входитиме:

підтвердження деталей: особа, яка перевіряє факти, повинна мати змогу підтвердити деталі з незалежних джерел;

виправлення неточностей в інформаційних повідомленнях (якщо такі неточності не спотворюють початковий зміст інформації);

обґрунтування чи спростування гіпотез. Гіпотези висуваються у тому випадку, якщо інформація не має прямих структурно-логічних зв'язків.

підтвердження джерел інформації: імена, адреси та особисті дані цитованих джерел повинні бути підтверджені, включаючи підтвердження того, що вони дійсно говорили або мали на увазі.

Загальна організаційна структура системи забезпечення достовірності інформації в організації може бути представлена наступною схемою (рис. 4.7).

Рис. 4.7. Організаційна структура системи забезпечення достовірності інформації в організації

Рекомендації щодо раціональної організації процесу оцінки достовірності інформації.

При сприйнятті, розумінні і подальшої інтерпретації важливої інформації, яка може впливати на процеси прийняття рішень, слід звертати увагу на такі показники.

1. Тип та ідеологія джерел/каналів (урядові, нейтральні, опозиційні, масові, ділові і розважальні та ін.), які відрізняються (від інших видань) картиною світу через підбір відповідних фактів і оцінок.

2. Наміри повідомлення, які можуть бути націлені на зміну типу поведінки, емоційно-експресивний вплив, художню обробку фактів, замовчування, маніпуляцію, дискредитацію, розвагу. Подібні прийоми цілком можуть свідчити про недостовірність (або неповну достовірність) повідомлення.

3. Імена рубрик та жанрів, що визначають шлях сприйняття інформації: хроніка, новини, аналітика, утилітарні жанри (донос, наклеп, плітки, газетна «качка», комплімент, хвастощі, імідж), гедоністичні жанри (байки, життєва історія, анекдот, легенда, нарисові і сатиричні форми і т.д.

4. Можливість верифікації інформації, достовірність якої встановлюється шляхом порівняння з даними, отриманими з альтернативних джерел (інших ЗМІ, незалежних джерел, свідчень учасників події, додаткових даних).

5. Надійність і авторитетність джерела (якісні ЗМІ, великі інформаційні агентства, офіційні матеріали, документи, експерти), з їх повної атрибуцією в тексті і посиланням на конкретне джерело. Анонімні, неназвані, невизначені джерела повинні насторожити і викликати сумнів в достовірності інформації.

6. Типи і види інформації. У повідомленнях використовуються різні типи інформації (факти, оцінки, нормативи, думки, гіпотези, прогнози, версії, фактоіди, чутки, байки, фейки; інформація «з других / третіх рук»), що займають на шкалі достовірності різні позиції. Саме фактологічна інформація локалізує подію в часі і просторі, встановлює його межі, пропонуючи аудиторії об'єктивну версію події.

7. Смислова відповідність заголовка, змісту тексту, зображення. Якщо між ними відсутній зв'язок, то виникають підстави засумніватися в достовірності джерела інформації, а також самого повідомлення. Розбалансування між компонентами тексту часто зустрічається в Інтернеті або «жовтих виданнях».

8. Мовні показники достовірності, які можуть підвищувати або знижувати ступінь достовірності повідомлення, тому треба вміти адекватно вичитувати смисли з комплексу багатоярусних слів-верифікаторів. Мовні інструменти дозволяють встановити відповідність сказаного дійсному стану справ і визначити позицію автора (впевненого, категоричного, сумнівається, що пом'якшує форму мови і ін.).

Загальна схема перевірки джерела інформації може мати вигляд, наведений на рис. 4.8.

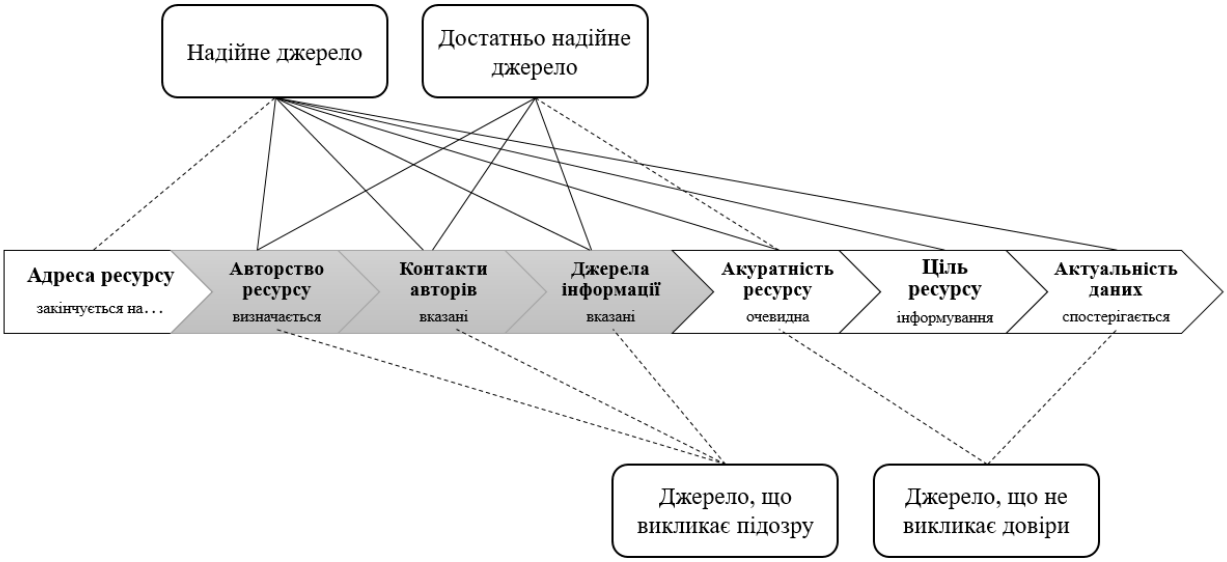

Рис. 4.8. Схема перевірки джерела інформації

Рекомендації щодо технічного забезпечення контролю достовірності інформації. Зважаючи на дедалі більшу популярність онлайн інформаційних ресурсів рекомендації щодо технічного забезпечення контролю достовірності зводяться до застосування програмних засобів перевірки. На теперішній час IT індустрія пропонує широкий вибір інструментів, які дозволяють організувати якісний факт-чекінг.

Botometer – сайт, який оцінює акаунти за шкалою від одного до п'яти, де один означає, что обліковій запис належить реальним користувачам, а п'ятіркою позначаються фейкові акаунти. Оцінка проводиться на основі твітів, історії публікацій та згадок іншими користувачами.

Detecting Fake News – програма на основі машинного навчання і байєсівських моделей для пошуку фейковий новин.

FactCheck.org – веб сайт, на якому користувачі можуть задавати питання про достовірність інформації, що звучить в заявах політиків, а команда сайту проводить розслідування і пропонує докладне пояснення. Пояснення включає інформацію про те, ким була зроблена заява, коли воно прозвучало і як

команда його перевіряла. У сайту також є спеціальна функція для перевірки наукової інформації - SciCheck.

Fake Bananas – програма на основі технологій машинного навчання. Шукає в авторитетних онлайн-виданнях статті, пов'язані з темою висловлювання, яке потрібно перевірити, і аналізує, чи згодні автори статей до укладеного в висловлюванні твердженням. Якщо достовірні джерела згодні з ним, програма оцінює затвердження як правдиве.

Genius – онлайн-ресурс «розподіленого фактчекінгу», який дозволяє завантажувати посилання на той чи інший матеріал і пропонує оцінити цей текст іншим користувачам.

Hoaxy – онлайновий інструмент, що візуалізує поширення статей в Інтернет. Орієнтований на перевірку фейкових новин сайт створює кольорові інтерактивні графіки, даючи користувачам можливість побачити, як різні заяви поширюються в Twitter.

Lazy Truth – додаток, покликаний допомогти користувачам визначити, які листи, що надходять в електронну скриньку, правдиві, а які – «міські історії» або спроба «розводу».

Politifact – веб сайт для перевірки заяв політиків і блогерів та оцінки цих тверджень за шкалою від "правда" до "відверта брехня".

Skeptive – сайт для визначення того, що правда, а що ні, на основі думок користувачів. Сервіс перевіряє, яку зі сторін спору підтримує найбільша кількість третіх джерел. Метою сервісу є максимально ефективне вирішення онлайн-суперечок.

Snopes – веб сайт для перевірки достовірності заяв, статей, постів в соціальних медіа та фотографій. Не обмежуючись простими заявами - "правда" або "брехня", Snopes використовує більш детальні категорії: "правда", "брехня", "суміш того й іншого", "в основному правда", "в основному брехня", "застаріла інформація", "неправильно зрозуміла

інформація" та ін. На сайті також можна знайти список сайтів, що поширюють фейковий новини.

Storyful Multisearch – інструмент для перевірки контенту з соціальних мереж. Пошук ведеться за ключовими словами одночасно у декількох соцмережах – Twitter, YouTube, Tumblr, Instagram і Spokeo.

Trooclick – інструмент, який сканує текст і, в разі якщо якийсь факт в статті не збігається з повідомленнями в інших ЗМІ або з офіційними статистичними даними, на екрані з'являється попередження: «Розбіжність із засобами масової інформації», «Розбіжність з офіційними документами», «Порушення журналістської етики». Крім того, користувачі можуть голосувати за статтю, натискаючи «так» або «ні» у відповідь на запитання: «Чи заслуговує довіри ця стаття?».

Truth Goggles – сайт дозволяє читачеві робити анотації в тексті: можна завантажити на сторінку текст або посилання на текст і звернути увагу на спірні моменти. Виділивши відрізок тексту, який заслуговує на увагу, користувач може вибрати, яке питання повинні задати собі інші читачі при його прочитанні. Наприклад: «Це дійсно так?» «Хто так сказав?» «Хто ще в цьому замішаний?» «Хто отримує від цього вигоду?» «Що ще варто про це знати?» і т.д.

Таким чином, використання технічних засобів оцінювання достовірності дасть змогу зменшити обсяг ручної роботи та час на перевірку джерел інформації.

Висновки до розділу 4

1. Перевірку істинності одержаних наукових результатів та загальної ефективності методики оцінки достовірності інформації найбільш доцільно

провести шляхом моделювання процесів забезпечення достовірності на прикладі типової компанії. При цьому слід вважати, що компанія для прийняття рішень потребує інформації з різних джерел та перебуває під впливом факторів інформаційного протиборства. Завданням керівництва та персоналу організації є використання лише достовірної інформації, для чого організується система забезпечення достовірності інформації, яка отримується з різних джерел.

2. Оцінювання ефективності одержаних теоретичних результатів здійснюється експертним методом, для чого інформаційні ресурси та канали інформаційного впливу ранжуються за ступенем впливу на рішення, що приймаються. Встановлюється ступінь впливу факторів інформаційного протиборства на інформаційні ресурси, вартість інформаційних ресурсів та визначається збиток, який може бути нанесений організації факторами інформаційного протиборства.

3. Результати експерименту показують, що показники достовірності половини ресурсів типової організації є нижчими рівня 0,5, що в контексті нечітких оцінок відповідає опису «недостовірно». При цьому найбільш цінні інформаційні ресурси захищені від дії факторів інформаційного протиборства відносно добре (достовірність більше 0,5).

4. Проведення заходів щодо забезпечення необхідного рівня достовірності дозволяє підвищити достовірність ресурсів за рахунок: підвищення адекватності моделей подання даних на 9–11%; підвищення якості організації інформаційного обміну на 6–8%; підвищення якості процедур контролю інформаційних ресурсів на 15–17%; підвищення кваліфікації персоналу на 17–19%.

5. Заходи щодо підвищення достовірності інформації можуть бути проведені за трьома напрямами: 1) побудова системи забезпечення достовірності інформації в організації (або шляхом створення окремого підрозділу чи призначення посадової особи, або шляхом розподілу обов’язків

щодо контролю достовірності інформації між різними посадовими особами за напрямами діяльності); 2) раціональна організація процесу оцінки достовірності; 3) технічне забезпечення контролю достовірності з використанням програмних комплексів.

ВИСНОВКИ

В результаті дисертаційних досліджень, виконаних автором, вирішено актуальне наукове завдання, що полягає у розробці методики оцінювання достовірності інформації в умовах інформаційного протиборства для захисту інформаційних ресурсів організації та забезпечення інформаційної безпеки користувачів. Зазначене наукове завдання має суттєве значення для захисту підприємств, організацій, їх працівників та виробничих процесів від зовнішніх і внутрішніх загроз в інформаційній сфері, а також підвищення ефективності функціонування інформаційних систем організацій в сучасних умовах. Відсутність аналогічних рішень у нашій країні та за кордоном робить результати досліджень пріоритетними.

В дисертації одержані такі основні наукові результати:

1. На підставі проведеного аналізу існуючих методичних підходів щодо оцінювання достовірності інформації в умовах інформаційного протиборства визначено, що основне протиріччя, яке лежить в основі наукового дослідження полягає, з одного боку в тому, що інформація, яка добувається, передається та зберігається, не завжди може бути представлена у вигляді даних чи відомостей на машинних носіях у стандартизованому чи формалізованому вигляді, а, відтак, потребує особливих підходів щодо її захисту від спотворення. З іншого боку, вплив інформаційного протиборства, який також є інформаційним, також не може бути представленим методами формальних теорій та числень, що унеможливлює його оцінювання під час оцінки достовірності інформації. Відтак, актуальним є наукове завдання щодо щодо розроблення методики оцінювання достовірності інформації в умовах інформаційного протиборства.

2. Удосконалено математичну модель інформаційного впливу, яка базується на системі диференційних рівнянь, що описують зміну кількості прихильників інформаційних повідомлень у залежності від індивідуальних

особливостей соціальних груп та, на відміну від існуючих, додатково враховує можливість забування та особливості засвоєння інформації окремими індивідами групи. Такий підхід дозволяє моделювати вплив на інформацію у процесі її проходження через різні засоби передачі та відтворювати процеси інформаційного протиборства при проходженні повідомлень від першоджерела до кінцевого користувача.

3. Вперше розроблено модель процесу управління достовірністю інформації в умовах інформаційного протиборства, яка базується на моделі скінченного автомата із заданим кінцевим станом достовірності інформаційних повідомлень при відомому початковому стані інформаційних ресурсів і наборові допустимих дій. Такий підхід дає можливість реалізувати багатокрокову перевірку повідомлень з поступовим підвищенням показників достовірності у залежності від характеру повідомлень та ступеня впливу на їх зміст.

4. Удосконалено методику оцінки достовірності інформації в умовах інформаційного протиборства, яка базується на методі експертного оцінювання та, на відміну від існуючих, додатково враховує частоту виникнення факторів інформаційного протиборства та ймовірність спроб порушення достовірності інформації. Така методика дозволяє визначати кількісні та якісні показники достовірності інформації в інформаційному потоці в умовах впливів, які можуть описуватися як чіткими так і нечіткими змінними.

5. Вперше розроблено методику оцінки ризиків порушення достовірності інформації, яка передбачає встановлення залежності можливого збитку організації через порушення достовірності вхідної інформації від ступеня впливу конкретного фактора інформаційного протиборства на окремий інформаційний ресурс. Такий підхід дозволяє визначати найбільш доцільні заходи щодо забезпечення достовірності інформації, яка надається такими ресурсами кінцевим споживачам.

6. Реалізація одержаних в дисертації наукових результатів дозволяє: сформувати підґрунтя для створення системи захисту інформації на підприємстві чи організації в умовах інформаційного протиборства; розробити комплекс алгоритмів перевірки достовірності інформації, які дозволяють сформувати систему управління інформаційним захистом підприємства на основі реалізації процедур управління достовірністю інформації; розробити рекомендації щодо удосконалення політик безпеки для організацій різних форм власності, які функціонують в умовах інформаційного протиборства з боку конкурентів та недоброзичливців.

7. Результати математичного моделювання та проведення практичного експерименту щодо створення системи забезпечення достовірності інформації у типовій організації дали можливість оцінити ефективність впровадження одержаних наукових результатів стосовно підвищення достовірності ресурсів за рахунок: підвищення адекватності моделей подання даних на 9–11%; підвищення якості організації інформаційного обміну на 6–8%; підвищення якості процедур контролю інформаційних ресурсів на 15–17%; підвищення кваліфікації персоналу на 17–19%.

8. Достовірність одержаних результатів підтверджується коректним використанням математичного апарату, обґрунтованими теоретичними твердженнями та апробацією математичних моделей і методів на тестових прикладах, які показують достатню збіжність аналітичних та експериментальних досліджень з результатами експертного оцінювання.

9. Мета досліджень, яка полягає у підвищенні достовірності інформації, яка передається від першоджерела до користувача в умовах інформаційного протиборства, досягнута і всі часткові завдання вирішено повністю. Наукові результати дисертаційного дослідження є внеском у розвиток методик та інструментарію оцінки стану інформаційної безпеки підприємств та організацій, як складової інформаційної безпеки держави, а

також концептуальних напрямів, організаційно-технічних підходів та заходів, покликаних попереджувати пошкодження їх інформаційних ресурсів.

10. Результати досліджень реалізовані у практичній діяльності в ТОВ «ІТ Спеціаліст» (акт від 09.12.2020 р.), в ТОВ «Євротелеком» (акт від 07.12.2020 р.).

11. Перспективними шляхами подальших досліджень у зазначеному напрямку може бути широке коло питань щодо розробки нових та удосконалення існуючих методів і методик виявлення загроз інформаційній безпеці підприємства чи організації, протидії негативному інфомаційному впливу та захисту інформаційних ресурсів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Бурячок, В. Політика інформаційної безпеки: підручник / В. Л. Бурячок, Р. В. Грищук, В. О. Хорошко; під заг. ред. проф. В. О. Хорошка. – К.: ПВП «Задруга», 2014. — 222 с.

2 Пузняк З.М. Методика виявлення впливу на достовірність інформації в інформаційному просторі / З.М. Пузняк, Д.А. Шеремет // Сучасний захист інформації. 2017. - №3. – С.50-55;

3 Пузняк З.М. Інформаційно-орієнтована модель як реалізація методики виявлення впливу на достовірність інформації в інформаційному просторі / З.М. Пузняк, А.О. Аносов // Сучасний захист інформації. 2017. - №4. – С.68-72;

4 Пузняк З.М. Дослідження процесу акустоелектричного перетворення в охоронних датчиках / З.М. Пузняк, М.В. Бржевський // Сучасний захист інформації. 2018. - №2. – С.65-71.

5 Бржевська З.М. Вплив на достовірність інформації як загроза для інформаційного простору / З.М. Бржевська, Г.І. Гайдур, А.О. Аносов // Кібербезпека: освіта, наука, техніка. – 2018. - №2(2). – С. 105-112. (Index Copernicus) DOI: 10.28925/2663-4023.2018.2.105112.

6 Бржевська З.М. Побудова системи маршрутизації даних в безпроводових сенсорних мережах на основі концепції лавинного розповсюдження (flooding) / Н.М. Довженко, Р.В. Киричок, З.М. Бржевська // Сучасний захист інформації. №4 (36), 2018., С. 17-21 DOI: 10.31673/2409-7292.2018.041216

7 Бржевська З.М. Інформаційні війни: проблеми, загрози та протидія / З.М. Бржевська, Н.М. Довженко, Р.В. Киричок, Г.І. Гайдур, А.О. Аносов // Кібербезпека: освіта, наука, техніка. – 2019. - №3(3). – С. 88-96. (Index Copernicus) DOI: 10.28925/2663-4023.2019.3.8896.

8 Бржевська З. Дослідження проблематики функціонування алгоритму передачі інформації при наявносі прихованих вузлів в безпроводових сенсорних мережах / А. Бондарчук, З. Бржевська, Н. Довженко, А. Макаренко, В. Собчук // Кібербезпека: освіта, наука, техніка. – Том 4 № 4., 2019. – С. 54-61 (Index Copernicus) DOI 10.28925/2663-4023.2019.4.5461

9 Бржевська З. Критерії моніторингу достовірності інформації в інформаційному просторі / З. Бржевська, Н. Довженко, Г. Гайдур, А. Аносов // Кібербезпека: освіта, наука, техніка. – Том 1 № 5., 2019. – С. 52-60. (Index Copernicus) DOI 10.28925/2663-4023.2019.5.5260

10 Brzhevska Z. Analysis and design of a hybrid load management method for the IoT networks / Vitalii Savchenko, Volodymir Druzhynin, Mykola Tverdohlib, Yevhen Ivanichenko, Nadiia Dovzhenko, Zoreslava Brzhevska, Valentina Chorna. // International Journal of Advanced Trends in Computer Science and Engineering, 9(1), January – February 2020. – (Scopus Indexed) - ISSN. 2278-3091, P 552 – 557

11 Бржевська З.М. Вплив на достовірність як загроза для інформації. – Ч Всеукраїнська науково-практична конференція «Актуальні проблеми управління інформаційною безпекою держави». – Збірник тез наукових доповідей Національної академії служби безпеки України. м. Київ, 4 квітня 2019р. – С. 282 - 284

12 Бржевська З.М. Аналіз класифікацій загроз інформаційній безпеці держави. – Всеукраїнська наукова конференція: «Актуальні проблеми кібербезпеки». – Збірник наукових тез наукових доповідей Державного університету телекомунікацій. м. Київ, 24 жовтня 2019р. – С. 27-28

13 Теоретичні підходи до вивчення інформаційного простору [Електронний ресурс] // Лекции. нет. – Режим доступу: http://lektsii.net/1-96772.html

14 Тенденції розвитку системи інформаційної безпеки України [Електронний ресурс] // Библиофонд. – Режим доступу: http://bibliofond.ru/view.aspx?id=652263

15 Поняття інформаційного простору [Електронний ресурс] // Навчальні матеріали онлайн. – Режим доступу: http://pidruchniki.-com/1350052747708/informatika/ponyattya_-informatsiynogo_prostoruyu/

16 Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Монография. — СПб.: Наукоемкие технологии, 2017. — 546 с.

17 Шушатський А. Аналіз підходів впливу засобів радіоелектронного подавлення на мережецентричну систему управління / О. Сова, Ю. Журавський, О. Налапко, Ю. Сокіл, Ю. Риндін // Системи управління, навігації та звязку. - №6(58), 2019. - С. 129-139

18 Антонович П. И. Изменение взглядов на информационное противоборство на современном этапе // Вестник Академии военных наук. 2011. № 1 (34). С. 43-47.

19 Груздева Л.М. О задаче повышения производительности интегрированной АСУ в условиях воздействия дестабилизирующих факторов / Л.М. Груздева // Международный журнал экпериментального образования №11, 2015. - С. 446-448

20 Ковалев В.А. Разработка информационной системы формирования рабочих программ и фондов оценочных средств / В.А. Ковалев, С.Ю. Пестова // Прикладная информатика в информационной сфере, 2015. - С. 29-36

21 Юдін О.К., Бучик С.С. Державні інформаційні ресурси. Методологія побудови класифікатора загроз. - К. НАУ, 2015. - 212 с.

22 Абрамов К.Г., Монахов Ю.М. Стохастические модели распространения нежелательной информации в социальных сетях// Сборник научных трудов Sworld. 2011. Т.5(4). С. 42-45.

23 Кузнецова А.П. Репутация Интернет-источников данных в информационно-аналитической деятельности администратора безопасности / А.П. Кузнецова, Г.Е. Монахова, М.Ю. Монахов // Динамика сложніх систем - XXI век Т.10, №4, 2016. С.78-81

24 Жилин Д.М. Теория систем. М.: УРСС, 2004. 183 с.

25 Erwin Folmer, Jack Verhoosel State of the Art on Semantic IS Standardization, Interoperability & Quality. University of Twente, 2011. 167 p.

26 Монахов Ю.М., Семенова И.И., Медведникова М.А., Костина Н.В. Методика выявления семантических дифференциалов для автоматизации оценки психосемантического профиля пользователя социальной сети // Современные проблемы науки и образования. 2013. № 5. URL: http://www.science-education.ru/111-10320

27 Gruzdeva L.M., Monakhov M.Yu. Early detection algorithm for at-tacks against information resources of automatic manufacturing control systems // Automation and Remote Control. 2011. V. 72. № 5. P. 1075-1079.

28 Семенова И.И. Аспекты информационной безопасности в системах управления базами моделей // МИК-2012. Омск: Правительство Омской области, 2012. С. 246-252.

29 Сотник В. Методика відбору критичних технологій / Расстригін О., Купчин А. // Information and analytical activities in the field of security and defense № 1(37), 2020. С. 67-76

30 Пєвцов Г. В. Інформаційно-психологічні операції Російської Федерації в Україні: моделі впливу та напрями протидії / Г.В. Пєвцов, С.В. Залкін, С.О. Сідченко, К.І. Хударковський // Наука і оборона №2, 2015. С. 28-32

31 Додонов В.О. Інформаційні технології аналізу та виявлення інформаційного впливу в соціальних мережах на основі мультиагентних моделей розповсюдження інформації. Дисертація. - К.: ДУТ, 2017. - 143 с.

32 Гриб Д.А. Принципи, методи і технології ведення збройної боротьби, управління силами і засобами в умовах активного інформаційного протиборства конфліктуючих сторін / Д.А. Гриб, Б.О. Демідов, Ю.Ф. Кучеренко, А.М. Ткачов, Т.В. Кулєшова // Наука і техніка Повітряних Збройних Сил України, №1(34), 2019. С. 12-22

33 J. Debattista, S. Auer, Ch. Lange A Methodology and Framework for Linked Data Quality Assessment // Journal of Data and Information Quality Vol.8 No.1, 2016. P. 21-32

34 A. Schiller, B. Heinrich, D. Hristova, M. Klier, M. Szubartowicz Requirements for Data Quality Metrics // Journal of Data and Information Quality Vol.9 No.2, 2018. P. 21-32

35 Ruzaini, Abdullah Arshah and Mohd Zafrol, Abdullah (2018) A Review of Data Quality Assessment: Data Quality Dimensions from User's Perspective. Advanced Science Letters, 24 (10). pp. 7824-7829. ISSN 1936-6612

36 The Next Frontier for Scalable Additive Manufacturing? Additive MES Software 20 Apr 2018. Режим доступу: https://amfg.ai/2018/04/20/am-automation-software-the-next-frontier/

37 Андреев А., Казаков Г.В., Коряков В. В. Метод оценки показателя достоверности выходных данных, подготавливаемых средствами автоматизированной системы подготовки данных полета летательных аппаратов // Инженерный журнал: наука и инновации. №4, 2019. С. 1-18

38 C. Batini, M. Scannapieco Data and Information Quality. Springer, 2016. 500 p.

39 Ge Peng, David Moroni, Chung-Lin Shie Ensuring and Improving Information Quality for Earth Science Data and Products // D-Lib Magazine, 2017. Vol.23 (7/8). P. 23-33

40 Sung-Eun Kim, Kyung Young Lee, Soo Il Shin, Sung-ByungYang Effects of tourism information quality in social media on destination image

formation: The case of Sina Weibo // Information & Management, 2017. Volume 54, Issue 6, Pages 687-702

41 Anna Mierzecka, Jacek Wasilewski and Małgorzata Kisilowska Cognitive authority, emotions and information quality evaluations // Proceedings of the Tenth International Conference on Conceptions of Library and Information Science, Ljubljana, Slovenia, June 16-19, 2019. Режим доступу: http://www.informationr.net/ir/24-4/colis/colis1910.html

42 Jee-Won Kangб Young Namkung The information quality and source credibility matter in customers' evaluation toward food O2O commerce // International Journal of Hospitality Management, 2019. Volume 78, Pages 189-198

43 Ismail Erkan, Chris Evans The influence of eWOM in social media on consumers' purchase intentions: An extended approach to information adoption // Computers in Human Behavior, 2016. Volume 61, Pages 47-55

44 Ashley Edelen, Wesley Weeks Ingwersen Guidance on Data Quality Assessment for Life Cycle Inventory Data / National Risk Management Research Laboratory Office of Research and Development, 2016. 37 p.

45 Юдін О.К., Ільєнко А.В. МЕТОДИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ КЕРУВАННЯ // О.К. Юдін, А.В. Ільєнко, Р.В. Зюбіна / Наукоемкие технологии в инфокоммуникациях: обработка информации, кибербезопасность, информационная борьба: Монография / под общей редакцией В. М. Безрука, В. В. Баранника. – Х.: Издательство «Лидер», 2017. 600 с. (с. 357-374)

46 Using information quality for the identification of relevant web data sources: a proposal / Bernadette Farias Lóscio, Maria C. M. Batista, Damires Souza, Ana Carolina Salgado // In Proceedings of the 14th International Confer-ence on Information Integration and Web-based Applications & Services (IIWAS '12). ACM, New York, NY, USA, 2012. P. 36-44.

47 Heiko Müller, Johann-Christoph Freytag, Ulf Leser Improving data quality by source analysis // J. Data and Information Quality. 2012. V. 2, № 4. 38 p.

48 Monika Krakowska Affective Factors in Human Information Behavior: A Conceptual Analysis of Interdisciplinary Research on Information Behavior. Wydawnictwa Uniwersytetu Warszawskiego, 2020. 95 p.

49 Stacie Petter, William DeLone, Ephraim R. McLean Information Systems Success: The Quest for the Independent Variables / Journal of Management Information Systems, 2014. Vol.29. p.7-62

50 Benjamin T. Hazen, Christopher A. Boone, Jeremy D. Ezell, L. Allison Jones-Farmer Data Quality for Data Science, Predictive Analytics, And Big Data In Supply Chain Management: An Introduction to The Problem And Suggestion For Research And Applications / International Journal of Prodution Economics, 2014. Vol.154. p. 72-80.

51 Ibrahim Abaker Targio Hashem, Ibrar Yaqoob The Rise of "Big Data" on Cloud Computing: Review and Open Research Issues / Information Systems, 2015. Vol.47. p. 98-115

52 McKenzie Raub Bots, Bias and Big Data: Artificial Intelligence, Algorithmic Bias and Disparate Impact Liability in Hiring Practies / Arkansas Law Review, 2018. Vol.71.Numb.2. p.529-570

53 Roman Lukyanenko, Jeffrey Parsons, Yolanda F. Wiersma The IQ of the Crowd: Understanding and Improving Information Quality in Structured User-Generated Content / Information System Research, 2014. Vol. 25, No. 4. p. 669–689

54 Bongsug (Kevin) Chae Insights from hashtag #supplychain and Twitter Analytics: Considering Twitter and Twitter data for supply chain practice and research / International Journal of Production Economics, 2015. Vol.165. p. 247-259

55 Borris Otto Quality and Value of the Data Resource in Large Enterprises / Information System Management, 2015. Vol. 32. p. 234-251

56 Using information quality for the identification of relevant web data sources: a proposal / Bernadette Farias Lóscio, Maria C. M. Batista, Damires Souza,

Ana Carolina Salgado // In Proceedings of the 14th International Confer-ence on Information Integration and Web-based Applications & Services (IIWAS '12). ACM, New York, NY, USA, 2012. P. 36-44.

57 Ohbyung Kwon, Namyeon Lee, Bongsik Shin Data Quality Management, Data Usage Experience and Acquisition Intention Of Big Data Analytics / International Journal of Information Management, 2014. Vol. 34. p. 387-394

58 Hefu Liu, Weiling Ke, Kwok Kee Wei, Zhongsheng Hua The Impact of IT Capabilities on Firm Perfomance: The Mediating Roles of Absorptive Capacity And Supply Chain Agility / Decision Support Systems, 2013. Vol.54. P. 1452-1462.

59 Adiska Fardani Haryadi, Joris Hulstijn Antecedents of Big Data Quality: An Empirical Examination In Financial Service Organizations / Proceedings of the IEEE International Conference on Big Data, 2016. P. 116-121

60 Hampapuram Ramapriyan, Ge Peng, David Moroni Ensuring and Improving Information Quality for Earth Science Data and Products / D-Lib Magazine, 2017. Vol.23 (7/8). P. 55-69

61 Xenia Papadomichelaki, Gregoris Mentzas e-GovQual: A Multiple-Item Scale for Assessing E-Government Service Quality / Government Information Quarterly, 2012. Vol. 29. P. 98-109

62 Arun Thotapalli Sundararaman Data Quality for Data Mining in Business Intelligence Applications: Current State and Research Directions // India: Accenture, 2015. 26 p.

63 A. Immonen, P Paakkonen, E Olavska Evaluating The Quality Of Social Media Data in Big Data Architecture // IEEE Access, 2015. Vol. 3. P. 2028-2043

64 O. Maimon, M. Last Knowledge Discovery and Data Mining: The Info-Fuzzy Network (IFN) Methodology // Springer, 2013. P.1003

65 Aimad Karkouch, Hajar Mousannif Data Quality In Internet of Things: A State-of-the-Art Survey / Journal of Network and Computer Applications, 2016. Vol.73. P.57-81

66 Jinjiang Wang, Yulin Ma Deep Learning For Smart Manufacturing: Methods and Applications / Journal of Manufacturing Systems, 2018. P/1-13

67 Meenakshi Jakhar, Sanjay Kumar Role of contextual factors in influencing user evaluation of information system: an analytic hierarchical process approach / International Journal of Bussines Information Systems, 2020. Vol.34. P. 25-44

68 Federico Costantini, Fausto Galvan Assessing "Information Quality" in IoT Forensics: Theretical Framework and Model Implemention / Journal of Applied Logics, 2020. P. 1-33

69 Mario Mezzanzanica, Roberto Boselli A Model-Based Evaluation of Data Quality Activities in KDD / Information Processinf & Management, 2015. Vol.51. P. 144-166

70 Nickolas J. Santero, Eric Masanet, Arpad Horvath Life-Cycle Assessment of Pavements. Part I: Critical Review / Resources, Conservation and Recycling, 2011. Vol. 55. P. 801-809.

71 Rupa Mahanti Critical Success Factors for Implementing Data Profiling: The First Step Toward Data Quality / Software Quality Professional, 2014. Vol.16. P.13-26

72 Barna Saha, Divesh Srivastava Data Quality: The Other Face of Big Data / IEEE 30th International Conference on Data Enineering, 2014. P.1-4

73 Roman Lukyanenko, Binny M. Samuel, Jeffrey Parsons Artifact Sampling: Using Multiple Information Technology Artifacts to Increase Research Rigor / Proceedings of the 51st Hawaii International Conference on System Sciences, 2018. P. 235-244

74 А.В. Дудатьєв, О.П. Войтович Інформаційна безпека соціотехнічних систем: модель інформаційного впливу // Інформаційні технології та компютерна інженерія, 2017. №10. С. 16-21

75 Маревцева Н.А., Валмуллин А.Н. Вычислительные эксперименты с моделями информационного противоборства // Математическое

моделирование социальных процессов. Вып. 14. М.: Макс-пресс, 2014. С. 62-80.

76 Е.В. Вайц Системно-динамическое моделирование процессов информационного противоборства // Интернет-журнал "Технологии техносферной безопасности", 2017. Выпуск №2 (72). С. 307-315

77 Михайлов А.П., Петров А.П., Маренцева Н.А., Третьякова И.В. Развитие модели распространения информации в социуме // Математическое моделирование. 2014. Т.26., №3. С. 65-74.

78 А.П. Михайлов, А.П. Петров, О.Г. Прончева Математическое моделирование информационного противоборства в эпоху Интернета // Труды XVIII Всероссийской конференции Научный сервис в сети Интернет, 2016. С. 264-270.

79 Using information quality for the identification of relevant web data sources: a proposal / Bernadette Farias Lóscio, Maria C.M. Batista, Damires Souza, Ana Carolina Salgado // IIWAS '12. ACM, NY, USA, 2012. P. 36-44.

80 Юдін О.К., Бучик С.С. Концептуальний аналіз уразливості державних інформаційних ресурсів // Наукоємні технології. – 2013. – № 3(19). – (Технічні науки). – С. 299-304

81 Приймак Ю.Ю. Національні інформаційні ресурси – джерело державних інформаційних продуктів та послуг // Державне управління: теорія та практика. – 2009. – № 2. – Режим доступу: http://www.academy.gov.ua/ej/ej10/doc_pdf/Priymak.pdf

82 А.В. Дудатьєв Інформаційна обфускація: Методи і моделі // Сучасний захист інформації, 2015. №4. С. 56-61

83 В.В. Козик, Ю.І. Сидоров Проблеми застосування моделей типу "хижак-жертва" в економічній практиці // Наука та інновації, 2011. Т.7. №1. С. 5-15

84 Сухарев М.С., Монахов Ю.М. Модель оценки функциональной устойчивости бизнес-процессов // Вестник Костромского государственного университета. 2011. №5-6. С. 4-6.

85 Сухарев М.С., Монахов Ю.М., Файман О.И. Применение системного подхода к оценке функциональной устойчивости бизнес – процессов // Сборник научных трудов Sworld. 2011. Т. 5. № 4. С. 70-73.

86 В.С. Кузнецов, В.Н. Кравченко Интегрированная модель системы маркетингово-ориентированного управления предприятием в сфере информационного бизнеса //Вісник Бердянського університету менеджменту і бізнесу, 2012. №3 (19). С. 91-95

87 Д.А. Полянский Математические основі управления информационной безопасностью. Управление статистическими показателями информационной безопасности. Учеб.пособие // Владимир: Владим. гос. ун-т. Владимир, 2020. 116 с.

88 ISO/IEC 15408-1:2009 – Information technol-ogy – Security techniques – Evaluation criteria for IT security – Part1: Introduction and general model. man-agement [Электронный ресурс]. – Режим доступа: http://www.iso.org/iso/catalogue_detail.htm?csnumber=50341

89 Мамончикова А.С. Формализация информационного конфликта на основе теории динамических систем // Наукоемкие технологии в космических иследованиях Земли, 2020. Т.12 №6. С. 68-75

90 Модели обеспечения достоверности и доступности информации в информационно-телекоммуникационных системах: монография / М. Ю. Монахов [и др.] ; Владим. гос. ун-т им. А. Г. и Н. Г. Сто-летовых. – Владимир: Изд-во ВлГУ, 2015. – 208 с

91 ISO/IEC 15408-2:2008 – Information technol-ogy – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements. [Электронный ресурс]. – Режим доступа:

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46414

92 ISO/IEC 15408-3:2008 – Information technol-ogy – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements. [Электронный ресурс]. – Режим доступа: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46413

93 Остапенко Г.А., Паринова Л.В., Белоножкин В.И., Батаронов И.Л. Информационные риски в социальных сетях. Монография // Воронеж: ООО "Издательство "Научная книга"", 2013. 159 с.

94 С.Ю. Борзенкова, Е.Е. Казарина Анализ методов уровня защищенности информационных систем в процессе их эксплуатации // Известия ТулГУ. Технические науки, 2020. Вып.5. С. 93-97

95 Полянский Д.А., Монахов М.Ю. Модель оценки факторов изменения достоверности информации в корпоративной сети передачи данных // Изв. ВУЗов. Приборостроение, 2012. Т.55 №8. С. 39-43

96 Ivan V. Sergienko Methods of Optimization and Systems Analysis for Problems of Transcomputational Complexity / Springer, 2012. 223 p.

97 Sebastian Behrendt, Alexander Richter Mixed methods analysis of enterprise social networks / Computer Networks, 2014. No.75. P. 560-577

98 Вентцель Е.С. Теория вероятностей. М.: Высшая школа, 2018. 576 с.

99 Семенова И.И. Управление процессом обеспечения достоверности информации в интеллектуальных системах поддержки принятия решений // Одиннадцатый Международный симпозиум "Интеллектуальные системы", 2014. С. 310-314

100 Иванова Н.В., Коробулина О.Ю. Аудит информационной безопасности. Учеб. Пособие // СПб: 2011. 57 с.

101 T. Butko, A. Prokhorchenko, M. Muzykin An Improved of Fetermining The Schemes of Locomotive Circulation with Regard to The Technological Peculiarities of Railcar Traffic // Eastern-European Journal of Enterprise Technologies, 2016. No. 5/3 (83). P. 47-55

102 Грищук Р. В. Основи кібернетичної безпеки: Монографія / Р.В. Грищук, Ю.Г. Даник; за заг. ред. проф. Ю.Г. Даника. – Житомир: ЖНАЕУ, 2016. – 636 с.

103 Н.Ю. Чорна, В.М. Коцюба Інноваційнийпідхід до моделювання бізнес-процесів // Вісник Хмельницького національного університету, 2011. №5. Т.1. С. 155-158

104 Г.В. Пєвцов, О.А. Усачова, П.Пацек, А.О. Романюк Комбінована методика оцінювання компетентності експертів привиборі сценарію організації інформаційно-психологічного впливу // Нака і техніка Повітряних Сил Збройних Сил України, 2020. №2(39). С. 24-36

105 Ю.М. Лисецкий Экспертные технологии в моделировании систем // Тринадцята Міжнародна науково-практична конференція "Математичне та імітаційне моделювання систем МОДС 2018", 2018. Тези доповідей. С. 288-292. Режим доступу: http://stu.cn.ua/media/files/conference/mods2018.pdf#page=288

106 Проничкин С.В., Раевская Е.Г., Тихонов И.П. Опіт организации и проведения комплексной єкспертизы результатов научно-технической программы // Химическая безопасность, 2017. Т.1. №2. С. 147-157.

107 Калашников А.О., Аникина Е.В. Управление информационными рисками сложной системы с использованием механизма "Когнитывной игры" // Вопросы кибербезопасности, 2020. №4 (38). С. 1-9

108 Жуков М.С., Орлов А.И., Фалько С.Г. Экспертные оценки в рисках // Контроллинг, 2017. № 66. С. 24-27.

109 Селезнев А.Д. Краткий обзор наиболее важных вопросов, связанных с составлением системы автоматизированного составления

расписания занятий в учебном заведеении // Advanced Science. Сборник статей III Международной научно-практической конференции, 2018. С. 74-76

110 Victoria Hemming, Mark A. Burgman A Practical Guide to Structured Expert Elicitation Using The IDEA Protocol // Methods in Ecology and Evolution, 2017. P. 169-180

111 Mahdi Bohlouli, Nikolaos Mittas, George Kakarontzas Competence Assessment as an Expert System for Human Resource Management: A Mathematical Approach // Journal of Expert Systems with Applications, 2017. P.1-36

112 Плетнев П.В., Белов В.М. Методика оценки рисков информационной безопасности на предприятиях малого и среднего бизнеса // Доклады ТУСУРа, 2012. №1 (25), часть 2. С. 83-86

113 Алексеев А.О., Калентьева А.С. Алгоритмические основы нечеткой процедуры комплексного оценивания объектов различной природы // Фундаментальные исследования. – 2014. – № 3 (часть 3) – С. 469-474

114 Сухарев М.С., Монахов Ю.М. Модель оценки функциональной устойчивости бизнес-процессов // Вестник КГУ им. Н.А. Некрасова, 2011. №5-6. С. 4-6

115 Кацупеев А.А. Анализ математических методов, применяемых для задач формирования информационной защиты распределенных систем // Сборник научных статей по материалам 15-ой Международной научно-практической конференции, 2015. С. 34-38

116 Виноградов И.М. Основы теории чисел. М.: Наука, 1981. 176 с.

117 A. Zh. Abdenov, V.A. Trushin, G.A. Abdenova Complex Method to Calculate Objective Assessments of Information System Protection to Improve Expert Assessments Reliability // Journal of Physics: Conference Series, 2018. P. 1-16.

118 Смыкова В.Н., Нечволода В.Э., Орёл Д.В. Экономические аспекты информационной безопасности // Сборник материалов X Всероссийской

научно-технической конференции с международным участием. 2019. С. 162-169.

119 Монахов М.Ю, Полянский Д.А., Монахов Ю.М., Семенова И.И. Концепция управления процессом обеспечения достоворнести информации в ИТКС в условиях информационного противодействия // Фундаментальные исследования. – 2014. – № 9 (часть 11) – С. 2397-2402

120 Монахов Ю.М., Груздева Л.М. Теоретическое и экспериментальное исследование распределенных телекоммуникационных систем в условиях войздействия вредоносных программ. Монография // Владимир, 2013. 132 с.

122 П.В. Комазов Використання методів нечітких множин у процесі ідентифікації економічного об'єкта // Бізнес Інформ, 2012. С. 55-58

123 Д. Назаров, Л. Конышева Интеллектуальные системы: основы теории нечетких множеств 3-е изд. // М.: Юрайт, 2019. 186 с.

124 Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Монография. — СПб.: Наукоемкие технологии, 2017. — 546 с.

ДОДАТОК А

ЗАТВЕРДЖУЮ
Директор ТОВ «ІТ Спеціаліст»
_____ Семєйкін Ю.Б.
«__9__» ___грудня___ 2020 року

АКТ

про впровадження результатів дисертаційного дослідження БРЖЕВСЬКОЇ Зореслави Михайлівни на тему: «Методика оцінки достовірності інформації в умовах інформаційного протиборства», поданої на здобуття наукового ступеня Доктора філософії за спеціальністю 125 – Кібербезпека

Даним актом засвідчено, що результати наукових досліджень дисертаційної роботи Бржевської Зореслави Михайлівни, були реалізовані при вдосконаленні системи забезпечення інформаційної безпеки Компанії.

Перелік реалізації та впровадження результатів дисертаційного дослідження:

1. Вперше розроблено методику оцінки ризиків порушення достовірності інформації, яка передбачає встановлення залежності можливого збитку організації через порушення достовірності вхідної інформації від ступеня впливу конкретного фактора інформаційного протиборства на окремий інформаційний ресурс. Такий підхід дозволяє визначати найбільш доцільні заходи щодо забезпечення достовірності інформації, яка надається такими ресурсами кінцевим споживачам.
2. Результати математичного моделювання та проведення практичного експерименту щодо створення системи забезпечення достовірності інформації в Компанії дали можливість оцінити ефективність впровадження одержаних наукових результатів стосовно підвищення достовірності ресурсів за рахунок: підвищення адекватності моделей подання даних на 9–11%; підвищення якості організації інформаційного обміну на 6–8%; підвищення якості процедур контролю інформаційних ресурсів на 15–17%; підвищення кваліфікації персоналу на 17–19%.

Наукові та практичні результати дослідження дозволяють сформувати підґрунтя для створення системи захисту інформації в Компанії в умовах інформаційного протиборства; розробити комплекс алгоритмів перевірки

достовірності інформації, які дозволяють сформувати систему управління інформаційним захистом Компанії на основі реалізації процедур управління достовірністю інформації; розробити рекомендації щодо удосконалення політик безпеки для організацій різних форм власності, які функціонують в умовах інформаційного протиборства з боку конкурентів.

Даний акт не є підставою для фінансових взаєморозрахунків.

Голова комісії:
Заступник директора з напрямку кібербезпеки Д.М. Петращук

Члени комісії:
Керівник відділу аудиту та сертифікації А.О. Журавльов
Керівник відділу
аналізу захищеності інформаційних систем А.Л. Панасюк

АКТ

про впровадження результатів дисертаційної роботи
БРЖЕВСЬКОЇ Зореслави Михайлівни

Даним актом засвідчено, що результати наукових досліджень дисертаційної роботи Бржевської Зореслави Михайлівни, були реалізовані при вдосконаленні системи забезпечення інформаційної безпеки підприємства.

Перелік реалізації та впровадження результатів дисертаційного дослідження:

1. Вперше розроблено модель процесу управління достовірністю інформації в умовах інформаційного протиборства, яка базується на моделі скінченного автомата із заданим кінцевим станом достовірності інформаційних повідомлень при відомому початковому стані інформаційних ресурсів і наборові допустимих дій.

2. Достовірність одержаних результатів підтверджується коректним використанням математичного апарату, обґрунтованими теоретичними твердженнями та апробацією математичних моделей і методів на тестових прикладах, які показують достатню збіжність аналітичних та експериментальних досліджень з результатами експертного оцінювання.

Запропонована модель дає можливість реалізувати багатокрокову перевірку повідомлень з поступовим підвищенням показників достовірності у залежності від характеру повідомлень та ступеня впливу на їх зміст.

Даний акт не є підставою для фінансових взаєморозрахунків.

Директор ТОВ «ЄВРОТЕЛЕКОМ» **Павло Булавін**

«07» грудня 2020 року

ДОДАТОК Б

Наукові праці, у яких опубліковані основні наукові результати дисертації:

1. *Пузняк З.М.* Методика виявлення впливу на достовірність інформації в інформаційному просторі / З.М. Пузняк, Д.А. Шеремет // Сучасний захист інформації. 2017. - №3. – С.50-55;

2. *Пузняк З.М.* Інформаційно-орієнтована модель як реалізація методики виявлення впливу на достовірність інформації в інформаційному просторі / З.М. Пузняк, А.О. Аносов // Сучасний захист інформації. 2017. - №4. – С.68-72;

3. *Пузняк З.М.* Дослідження процесу акустоелектричного перетворення в охоронних датчиках / З.М. Пузняк, М.В. Бржевський // Сучасний захист інформації. 2018. - №2. – С.65-71.

4. *Бржевська З.М.* Вплив на достовірність інформації як загроза для інформаційного простору / З.М. Бржевська, Г.І. Гайдур, А.О. Аносов // Кібербезпека: освіта, наука, техніка. – 2018. - №2(2). – С. 105-112. (Index Copernicus) DOI: 10.28925/2663-4023.2018.2.105112.

5. *Бржевська З.М.* Побудова системи маршрутизації даних в безпроводових сенсорних мережах на основі концепції лавинного розповсюдження (flooding) / Н.М. Довженко, Р.В. Киричок, З.М. Бржевська // Сучасний захист інформації. №4 (36), 2018., С. 17-21 DOI: 10.31673/2409-7292.2018.041216

6. *Бржевська З.М.* Інформаційні війни: проблеми, загрози та протидія / З.М. Бржевська, Н.М. Довженко, Р.В. Киричок, Г.І. Гайдур, А.О. Аносов // Кібербезпека: освіта, наука, техніка. – 2019. - №3(3). – С. 88-96. (Index Copernicus) DOI: 10.28925/2663-4023.2019.3.8896.

7. *Бржевська З.* Дослідження проблематики функціонування алгоритму передачі інформації при наявності прихованих вузлів в

безпроводових сенсорних мережах / А. Бондарчук, З. Бржевська, Н. Довженко, А. Макаренко, В. Собчук // Кібербезпека: освіта, наука, техніка. – Том 4 № 4., 2019. – С. 54-61 (Index Copernicus) DOI 10.28925/2663-4023.2019.4.5461

8. *Бржевська З.* Критерії моніторингу достовірності інформації в інформаційному просторі / З. Бржевська, Н. Довженко, Г. Гайдур, А. Аносов // Кібербезпека: освіта, наука, техніка. – Том 1 № 5., 2019. – С. 52-60. (Index Copernicus) DOI 10.28925/2663-4023.2019.5.5260

9. *Brzhevska Z.* Analysis and design of a hybrid load management method for the IoT networks / Vitalii Savchenko, Volodymir Druzhynin, Mykola Tverdohlib, Yevhen Ivanichenko, Nadiia Dovzhenko, Zoreslava Brzhevska, Valentina Chorna. // International Journal of Advanced Trends in Computer Science and Engineering, 9(1), January – February 2020. – (Scopus Indexed) - ISSN. 2278-3091, P 552 – 557

10. *Бржевська З. М.* Метод контролю послідовності реалізації атакуючих дій під час активного аналізу захищеності корпоративних мереж / Р.В. Киричок, Г.В. Шуклін, З.М. Бржевська // Сучасний захист інформації. №2 (42), 2020., С. 52-58.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

11. *Бржевська З.М.* Вплив на достовірність як загроза для інформації. – Ч Всеукраїнська науково-практична конференція «Актуальні проблеми управління інформаційною безпекою держави». – Збірник тез наукових доповідей Національної академії служби безпеки України. м. Київ, 4 квітня 2019р. – С. 282 - 284

12. *Бржевська З.М.* Аналіз класифікацій загроз інформаційній безпеці держави. – Всеукраїнська наукова конференція: «Актуальні проблеми кібербезпеки». – Збірник наукових тез наукових доповідей Державного університету телекомунікацій. м. Київ, 24 жовтня 2019р. – С. 27-28

13. *Бржевська З.М.* Проблематика розвитку інформаційної безпеки в умовах інформаційного протиборства. – XII Всеукраїнська науково-практична конференція: «Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення. Застосування підрозділів, комплексів, засобів зв'язку, автоматизації та кібербезпеки в операції Об'єднаних сил». – Збірник наукових тез та доповідей Військового інституту телекомунікацій та інформатизації. м. Київ, 3 грудня 2020 р. - С. 104-105