МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ І ГЛОБАЛЬНОГО
ІНФОРМАЦІЙНОГО ПРОСТОРУ

Кваліфікаційна наукова праця
на правах рукопису

КУЗЬМЕНКО Лідія Володимирівна

УДК 681.5(042.3)

ДИСЕРТАЦІЯ

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ДЛЯ СТВОРЕННЯ ПЕРСПЕКТИВНИХ ГАРАНТОЗДАТНИХ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ ОБ'ЄКТАМИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Спеціальність 05.13.06 – Інформаційні технології

Технічні науки

Подається на здобуття наукового ступеня кандидата технічних наук

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

Л.В.Кузьменко
(підпис, ініціали та прізвище здобувача)

Науковий керівник Г.М.Гулак, кандидат технічних наук, доцент

Київ – 2021

АНОТАЦІЯ

Кузьменко Л.В. Методи та моделі створення перспективних гарантоздатних автоматизованих систем управління об'єктами критичної інфраструктури. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 «Інформаційні технології». Інститут телекомунікацій і глобального інформаційного простору НАН України, Київ, 2021.

Дисертаційна робота присвячена вирішенню актуальної наукової задачі, що полягає в розробленні теоретичних і прикладних засад побудови інформаційної технології (ІТ) для створення перспективних гарантоздатних (ПГ) автоматизованих систем управління (АСУ) об'єктів критичної інфраструктури (ОКІ), а також визначення впливу на процеси функціонування таких систем антропогенних і техногенних втручань та загроз.

Об'єктом дослідження в роботі є процеси створення перспективних гарантоздатних АСУ та процеси функціонування таких систем в умовах впливу антропогенних і техногенних втручань та загроз. ***Предметом дослідження*** – інформаційна технологія, спрямована на формування типового варіанту побудови ПГ АСУ, а також визначення впливу загроз порушення цілісності, конфіденційності та доступності (ЦКД) на процеси функціонування такої системи.

Метою роботи є побудова інформаційної технології для створення перспективних гарантоздатних АСУ ОКІ України, здатних гарантовано надавати абонентам необхідні послуги та/або сервіси, яким в заданих режимах і умовах застосування з урахуванням стану захищеності таких систем від загроз порушення ЦКД можливо виправдано довіряти. Для досягнення поставленої мети в роботі:

досліджено можливі загрози та сформовано їх актуальну множину, а також множину уразливостей безпеці функціонування АСУ ОКІ;

розроблено часткову модель загроз безпеці ПГ АСУ ОКІ;

розроблено метод визначення впливу загроз на процеси функціонування перспективних гарантоздатних АСУ ОКІ;

вдосконалено метод формування типового варіанту побудови перспективних гарантоздатних АСУ ОКІ.

Метод формування типового варіанту побудови ПГ АСУ ОКІ включає процедуру вибору прототипу топології мережевої інфраструктури, процедуру вибору типового АРМ раціональної конфігурації та процедуру раціонального вибору програмних засобів (ПЗ) прикладного рівня (ПР).

Вирішення задачі щодо вибору прототипу топології мережевої інфраструктури для побудови перспективної гарантоздатної АСУ ОКІ здійснюється в роботі двома способами. Перший з них ґрунтується на застосуванні класичних і похідних критеріїв прийняття рішень в умовах невизначеності – критеріях Вальда, Севіджа та надзвичайного оптимізму. Оскільки дані критерії надають практично ідентичні результати, рішення щодо обрання раціонального прототипу топології мережевої інфраструктури потребує уточнення. Тому в роботі було проведено додаткове дослідження, в основу якого покладено метод аналізу ієрархій. Застосування системної процедури ієрархічного представлення елементів АСУ ОКІ за критеріями вартості, функціональності і відповідності технічним вимогам з урахуванням місця і внеску показників, що відповідають кожному з цих критеріїв, дозволило створити передумови для організації доступу до мережі та надання обчислювальних ресурсів і послуг їх абонентам для спільного використання ІР загального користування, керування їх обміном, передачею, збереженням і поновленням та, на відміну від існуючих, приймати обґрунтовані рішення щодо обрання серед низки можливих варіантів прототипу топології мережевої інфраструктури АСУ ОКІ раціональної структури.

Вирішення задачі щодо вибору типового АРМ раціональної конфігурації для побудови перспективної гарантоздатної АСУ ОКІ ґрунтується на річній економії від впровадження АРМ та тих капіталовкладеннях, які витрачаються на їх впровадження. Річна економія в свою чергу залежить від приросту прибутків, що викликаний, наприклад, зменшенням фонду заробітної плати користувачів АРМ та змін, що можуть статися при впровадженні уніфікованого АРМ, наприклад, зменшення часу на підготовку документів через впровадження електронного документообігу. Капіталовкладення на впровадження АРМ складаються з витрат на придбання системного блоку, монітору, сканеру, принтеру, загального і спеціального програмного забезпечення. Такі витрати мають бути мінімальними. Як результат, врахування функціональності програмної та апаратної архітектури АРМ, а саме їх системності, гнучкості, стійкості, ефективності, ергономічності, тощо та реалізації нових ІТ у процесах виконання встановлених в АРМ функцій, дозволило забезпечити можливість доступу користувачам до власних і зовнішніх ІР та їх машинної обробки й, на відміну від існуючих, приймати обґрунтовані рішення щодо обрання серед низки можливих АРМ раціональної конфігурації.

Вирішення задачі щодо вибору програмних засобів (ПЗ) прикладного рівня (ПР) перспективної гарантоздатної АСУ ОКІ здійснюється за двома безрозмірними розрахунковими коефіцієнтами функціональності та раціональності. Коефіцієнт функціональності дозволяє врахувати при порівнянні ПЗ однакового

функціонального призначення такі функції, як застосування моделі даних, впровадження функціональних можливостей та забезпечення надійної експлуатації ПЗ. Кожна із цих функцій в свою чергу може бути реалізована одним із запропонованих в роботі варіантів. Їх поєднання здійснюється шляхом застосування технології морфологічних карт. За результатами опрацювання морфологічної карти обирається найбільш функціональний ПЗ з точки зору реалізації обраних функцій (критеріїв). За результатами подальшого рейтингування альтернативних рішень та багатокритеріального оцінювання їх якості за декількома частковими критеріями оптимальності приймається остаточне рішення щодо обрання найбільш результативного (раціонального) варіанту ПЗ.

Комплексним рішенням в межах вдосконаленого ***методу формування типового варіанту побудови ПГ АСУ ОКІ*** є процедура, що формується на підставі критеріїв, обчислених на попередніх етапах роботи та які найбільш повно характеризують конкретну АСУ ОКІ з точки зору її топології, архітектури (зокрема АРМ) та ПЗ, а також властивих для неї функцій й дозволяє обрати серед альтернативних варіантів побудови АСУ найкращий (раціональний).

Метод визначення впливу загроз на процеси функціонування перспективних гарантоздатних АСУ ОКІ включає семантичну модель протиборства системи захисту ПГ АСУ ОКІ з атакуючою стороною, процедуру детектування та відновлення даних в ПГ АСУ ОКІ та модель оцінки стану захищеності ПГ АСУ

Вирішення задачі протиборства системи захисту АСУ ОКІ та атакуючої сторони ґрунтується на процедурі потенційно можливого криптоперетворення інформації в системі. Її впровадження дозволило планувати заходи та обирати раціональні методи щодо відбиття нападу атакуючої сторони та нівелювання його наслідків й, на відміну від існуючих, відслідковувати вплив шкідливих програм, завідомо фальшивого ПЗ і злоякісних шифруючих кодів на інформаційно-технологічні процеси в АСУ ОКІ.

Вирішення задачі детектування та відновлення даних в АСУ ОКІ грунтується на технології кластерного аналізу, застосування якого дозволяє порівнювані дані поділити на групи так, щоб підзадачі усередині груп були подібні одна з одною, а підзадачі з різних груп суттєво відрізнялися. Як наслідок це дозволило розподілити множину задач на групи та сформувати деревоподібну ієрархічну структуру з певної кількості підзадач в кожній та в ході імітаційного експерименту дослідити можливості застосування кластерного аналізу для розпаралелювання процесів пошуку вразливостей або істинних значень ключів, застосованих для шифрування даних, а також оцінювання стійкості криптосистем від стороннього кібернетичного впливу та криптоперетворень. Отриманий результат суттєво залежатиме від таких факторів:

відсутності однозначно найкращого критерію якості кластеризації; невизначеності щодо попередньої кількості кластерів відносно деякого критерію; залежності результату кластеризації від міри близькості задач щодо відновлення зашифрованих даних, вибір якої також суб'єктивний і визначається експертом. Це, як результат, дозволяє створити передумови для оцінювання стійкості криптосистем.

Комплексним рішенням в межах розробленого ***методу визначення впливу загроз на процеси функціонування перспективних гарантоздатних АСУ ОКІ*** є модель оцінки стану захищеності перспективної гарантоздатної АСУ ОКІ від загроз порушення цілісності, конфіденційності та доступності яка, на відміну від подібних, дозволяє оцінювати події, що можуть впливати на ІТП ОКІ та прямо або опосередковано завдати збитку її власникам і користувачам, приймати обґрунтовані рішення щодо стану захищеності АСУ ОКІ від впливу кібернетичних атак та, як результат, убезпечити АСУ ОКІ від НСД до її ресурсів та інформації, що в ній циркулює.

У роботі проведено імітаційні експерименти щодо порівняльного оцінювання та вибору прототипу топології МІ, конфігурації АРМ та системи програмного забезпечення *ПГ АСУ ОКІ* прикладного рівня. В ході імітаційних експериментів у роботі досліджено можливості застосування кластерного аналізу для розпаралелювання процесів пошуку вразливостей або істинних значень ключів, застосованих для шифрування даних, а також оцінювання стійкості криптосистем від стороннього кібернетичного впливу та криптоперетворень.

Як наслідок, отримані в роботі наукові результати, утворюють у своїй сукупності ***інформаційну технології для створення перспективних гарантоздатних АСУ ОКІ***, впровадження якої, на відміну від існуючих, забезпечує гарантоване надання абонентам необхідних послуг та/або сервісів, яким в заданих режимах і умовах застосування з урахуванням стану захищеності таких систем від загроз порушення ЦКД можливо виправдано довіряти. Впровадження означеної ІТ окрім всього сприяє:

по-перше, підвищенню, за рахунок оперативного визначення серед множини можливих найбільш значимих загроз, результативності дій осіб, відповідальних за забезпечення безпеки ПГ АСУ ОКІ;

по-друге, скороченню часу на прийняття виважених управлінських рішень щодо побудови ПГ АСУ ОКІ.

Ключові слова: безпека, вплив, гарантоздатність, доступність, ефективність, засіб, комп'ютер, конфіденційність, критична інфраструктура, мережа, надійність, програма, прототип, цілісність, функціонал, система, топологія, управління

ABSTRACT

Kuzmenko LV Methods and models for creating the advanced guaranteed automated systems for managing critical infrastructure. – Manuscript.

The dissertation for the degree of a candidate of technical sciences on the specialty 05.13.06 "Information technologies." Institute of Telecommunications and Global Information Space of the National Academy of Sciences of Ukraine, Kyiv, 2021.

The dissertation work is devoted to the decision of an actual scientific problem consisting in development of theoretical and applied bases of construction of information technology (IT) for creation of perspective guaranteeable (GH) automated control systems (ACS) of objects of critical infrastructure (CIF), and also definition of influence on processes. functioning of such systems of anthropogenic and technogenic interventions and threats.

The object of research in this work are the processes of creating promising guaranteed ACS and the functioning of such systems under the influence of anthropogenic and man-made interventions and threats. The subject of the study is IT, aimed at forming a typical version of the construction of GHG ACS, as well as determining the impact of threats to integrity, confidentiality and accessibility (ICA) on the functioning of such a system. The purpose of the work is to build information technology to create promising warranty ACS CIF of Ukraine, able to provide subscribers with guaranteed necessary services and / or services, which in the given modes and conditions of application, taking into account the state of protection of such systems from threats of ICA justified to trust.

To achieve this goal in the work:

possible threats are investigated and their actual set, and also set of vulnerabilities of safety of functioning of ACS of CIF is formed;

developed a partial model of security threats to the GHG ACS;

developed a method for determining the impact of threats on the functioning of promising warranty ACS CIF;

the method of formation of a standard variant of construction of perspective guaranteeing ACS of CIF is improved.

The method of forming a typical variant of construction of GHG ACS includes the procedure of choosing a prototype topology of network infrastructure, the procedure of choosing a typical workstation of rational configuration and the procedure of rational choice of software (software) application level (AL).

The solution of the problem of choosing a prototype of the topology of the network infrastructure for the construction of a promising guarantee ACS OKI is carried out in two ways. The first of them is based on the application of classical and derivative decision-making criteria in conditions of uncertainty - the criteria of Wald, Savage and extreme optimism. It was impossible to choose a rational prototype of the network infrastructure topology according to these criteria, as they provided almost identical results. Therefore, an additional study was conducted in the work, which is based on the method of analysis of hierarchies. The application of a systematic procedure of hierarchical representation of the elements of ACS CIF on the criteria of cost, functionality and compliance with technical requirements, taking into account the place and contribution of indicators that meet each of these criteria, allowed to create conditions for organizing access to the network and providing computing resources and services to their subscribers public IR, managing their exchange, transmission, storage and renewal and, in contrast to existing ones, to make informed decisions on choosing among a number of possible variants of the prototype of the network infrastructure topology ACS CIF rational structure.

The solution of the problem of choosing a typical workstation of rational configuration for the construction of a promising warranty ACS CIF is based on annual savings from the introduction of workstations and those investments that are spent on their implementation. The annual savings in turn depend on the increase in income caused, for example, by the reduction of the salary fund of workstation users and changes that may occur with the introduction of a unified workstation, such as reducing the time to prepare documents through the introduction of electronic document management. Investments in the implementation of workstations consist of the cost of purchasing a system unit, monitor, scanner, printer, general and special software. Such costs should be kept to a minimum. As a result, taking into account the functionality of software and hardware architecture of workstations, namely their system, flexibility, stability, efficiency, ergonomics, etc. and the implementation of new IT in the process of performing functions installed in the workstation, allowed users to access their own and external IR and their machine processing and, in contrast to the existing ones, to make informed decisions on the choice of a rational configuration among a number of possible workstations.

The solution of the problem of rational choice of software of the application level (AP) of the promising warranty ACS CIF is carried out by two dimensionless calculation coefficients of functionality and rationality. The coefficient of

functionality allows taking into account when comparing software of the same functional purpose such functions as the application of the data model, the introduction of functionality and ensuring reliable operation of the software. Each of these functions in turn can be implemented by one of the options offered in the work. Their combination is carried out by applying the technology of morphological maps. Based on the results of morphological map processing, the most functional software is selected in terms of implementation of selected functions (criteria). Based on the results of further rating of alternative solutions and multi-criteria evaluation of their quality according to several partial criteria of optimality, the final decision is made on the selection of the most effective software option.

A comprehensive solution within the improved method of forming a typical version of the GHG ACS CIF is an approach that is formed on the basis of criteria calculated in previous stages of work and which most fully characterize a particular ACS CIF in terms of its topology, architecture (including workstations) and software, and also its inherent functions and allows you to choose among the alternatives for the construction of ACS the best (rational).

The method of determining the impact of threats on the functioning of promising warranty ACS CIF includes a semantic model of confrontation of the GHG ACS CIF protection system with the attacking party, an algorithm for detecting and recovering data in the GHG ACS CIF and a model for assessing the security of GHG ACS CIF.

The solution of the problem of confrontation between the security system of the ACS CIF and the attacking party is based on the procedure of potentially possible crypto-conversion of information in the system. Its implementation allowed to plan measures and choose rational methods to repel the attack of the attacking party and mitigate its consequences and, in contrast to existing ones, to monitor the impact of malware, knowingly fake software and malicious encryption codes on information technology processes in ACS CIF.

The solution of the problem of detection and recovery of data in ACS CIF is based on the technology of cluster analysis, the use of which allows comparable data to be divided into groups so that subtasks within groups were similar to each other, and subtasks from different groups differed significantly. As a result, it allowed to divide many tasks into groups and form a tree-like hierarchical structure of a number of subtasks in each and during the simulation experiment to explore the possibility of using cluster analysis to parallelize vulnerabilities or true key values used to encrypt data and evaluate stability. from external cybernetic influences and cryptocurrencies.

The obtained result will significantly depend on the following factors: the absence of clearly the best criterion for the quality of clustering; uncertainty about the previous number of clusters for a certain criterion; the dependence of the clustering result on the degree of proximity of the tasks for the recovery of encrypted data, the choice of which is also subjective and determined by the expert. As a result, it allows to create prerequisites for assessing the stability of cryptosystems.

A comprehensive solution within the developed method of determining the impact of threats on the operation of promising warranty ACS CIF is a model for assessing the state of protection of promising ACS CIF from threats of integrity, confidentiality and availability, which, in contrast, allows to assess events that may affect and directly or indirectly harm its owners and users, make informed decisions about the state of protection of ACS CIF from the impact of cyber attacks and, as a result, protect ACS CIF from unauthorized access (UHA) to its resources and information circulating in it.

The simulation experiments on the comparative evaluation and selection of the prototype of the MI topology, the configuration of the workstation and the software of the GHG ACS of the CIF of the applied level are carried out. The possibilities of application of cluster analysis for parallelization of processes of search of vulnerabilities or true values of keys used for data encryption, and also estimation of stability of cryptosystems from external cybernetic influence and cryptocurrencies are investigated in the work.

A comprehensive solution in the dissertation research is information technology to create promising guaranteed ACS CIF, the implementation of which, in contrast to existing: allows you to assess events that may affect the information and technological processes on the CIF and cause damage to both owners and users; provides guaranteed provision to subscribers of necessary services and / or services, which in the given modes and conditions of application, taking into account the state of protection of such systems from threats of violation of integrity, confidentiality and availability, may be reasonably trusted. The implementation of this IT also contributes to:

increase, due to the prompt identification of the set of possible most significant threats, the effectiveness of the actions of persons responsible for ensuring the safety of GHG ACS CIF;

reduction of time for making well-considered management decisions on the construction of GHG ACS CIF.

Keywords: security, impact, warranty, availability, efficiency, tool, computer, confidentiality, critical infrastructure, network, reliability, program, prototype, integrity, functionality, system, topology, management

СПИСОК ПРАЦЬ, ОПУБЛІКОВАНИХ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Колективна монографія в іноземному науковому виданні:

1. Dreis Y. A tuple model for estimating the consequences of personal data leakage in automated systems. VIII International conferece of students, PHD-students and young scientists «Engineer of XXI Century». /Y.Dreis, I.Lozova, A.Biskupskyi, **L.Kuzmenko,** Ali .T. Al-Khwalde, A.Korchenko // Processing, transmission and security of information. – Bielsku-Białej: NATH, 2018. Vol.2. – P. 41–50. ISBN: 978-83-65182-94-4.

2. Sokolov V. Development of low-budget spectrum analyzers for IOT and sensor networks. X International conferece of students, PHD- students and young scientists «Engineer of XXI Century». / V. Sokolov, A. Platonenko, **L. Kuzmenko**, V. Buriachok // Projektowanie, badania i eksploatacja. – Bielsku-Białej: NATH, 2020. – P. 331–342. ISBN: 978-83-66249-54-7.

Публікації у наукових фахових виданнях України:

3. Рейш О.Е., Бурячок В.Л., Вертегел С.Г., **Бурячок Л.В.** Методика вибору раціональної топології комп'ютерної мережі перспективних автоматизованих систем управління військами. Труди Академії. – К.: НАО МО України, 2009. – № 2(89). – С. 81–90.

4. Бурячок В.Л., **Бурячок Л.В.** Алгоритм порівняльного оцінювання програмних засобів однакового функціонального призначення для розв'язання завдань інформаційної діяльності. Збірник наукових праць. – К.: НДІ ГУР МО України, 2010. Вип. 27. – С. 124–139.

5. Бурячок В.Л., **Бурячок Л.В.,** Костюк Т.Я. Формування набору показників для оцінювання якості програмного забезпечення сучасних автоматизованих систем. Збірник наукових праць. – К.: НДІ ГУР МО України, 2010. Вип. 28. – С. 111–124.

6. Бурячок В.Л., **Бурячок Л.В.,** Гулак Г.М. Алгоритм вибору АРМ раціональної конфігурації. Сучасний захист інформації. – К.: ДУІКТ, 2011. – № 2. – С. 85–94.

7. Бурячок В.Л., **Бурячок Л.В.,** Костюк Т.Я. Обґрунтування вибору раціональної системи електронного документообігу для державних структур спеціального призначення. Вісник воєнної розвідки. – № 24. – 2011. – С. 67–74.

8.Козачок В.А., Бурячок В.Л., **Бурячок Л.В.,** Складанний П.М. Пентестінг, як інструмент комплексної оцінки ефективності захисту інформації в розподілених корпоративних мережах. Сучасний захист інформації. – К.: ДУТ, 2015. – № 3. – С. 4–12.

9. Бурячок В.Л., Невойт Я.В., **Бурячок Л.В.** Вплив загроз антропогенного і техногенного характеру на стан безпеки ІТ-систем та соціальних інститутів провідних країн світу і України. Сучасний захист інформації. – К.: ДУТ, 2015. – № 4. – С. 29–43.

10. **Бурячок Л.В.** Стратегія обґрунтування раціонального набору параметрів і функцій програмних засобів спеціального призначення, спрямованих на розв'язання завдань інформаційної діяльності. Сучасний захист інформації. – К.: ДУТ, 2016. – № 3. – С. 3–9.

11. **Бурячок Л.В.,** Бурячок В.Л., Семко В.В. Технологія проведення порівняльного аналізу та оцінювання стану захищеності автоматизованих інформаційних систем. Сучасний захист інформації. – К.: ДУТ, 2016. – № 4. – С. 16–24.

12. Козачок В.А., Рой Я.В., **Бурячок Л.В.** Технології протидії шкідливим програмам та завідомо фальшивому програмному забезпеченню. Сучасний захист інформації. – К.: ДУТ, 2017. – № 2(30). – С. 30–34.

13. V.L.Buryachok, **Kuzmenko L.V.,** Kononenko O.V., Boskin O.O. Features of implementation of the information security policy in the creation of the rational system of electronic documentary cooperation for public and commercial structures of Ukrain. Збірник наукових праць «Системні технології» Національної металургійної академії України. Том 6 (113) 2017. – С. 43–61

14. Гулак Г.М., Бурячок В.Л., Складаний П.М,. **Кузьменко Л.В.** Криптовірологія: загрози безпеки гарантоздатним інформаційним системам і заходи протидії шифрувальним вірусам. Кібербезпека: освіта, наука, техніка. Том 2. №10 (2020). – С. 6 – 28. ISSN 2663 – 4023

<u>Публікації у наукометричних базах Scopus і Web of Science:</u>

15. V. Lakhno, V. Malyukov, N. Mazur, **L. Kuzmenko,** B. Akhmetov. Development of a model for decision support systems for managing the process of investing in information technology. Східно-Європейський журнал передових технологій. ТОМ 1, № 3 (103) (2020), с. 74 – 81. ISSN (print) 1729-3774, ISSN (on-line) 1729-4061

16. Нашинець-Наумова А.Ю., В.Л. Бурячок, Н.В. Коршун, О.Б. Жильцов, П.М. Складанний, **Л.В. Кузьменко.** Технологія забезпечення інформаційної і кібербезпеки в закладах вищої освіти України. Електронне наукове фахове видання «Інформаційні технології і засоби навчання» Інституту інформаційних технологій і засобів навчання НАПН України. Том 77, № 4 (2020). – С. 337 – 354

17. Feodosiy Kipchuk, Volodymyr Sokolov, Volodymyr Buriachok, Pavlo Skladannyi, **Lidiia Kuzmenko.** Investigation of Availability of Wireless Access Points

based on Embedded Systems. Proceedings of the VI International Scientific and Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T'2019), October 8–11, 2019: abstracts. – Kyiv: IEEE, 2019. – P. 246–250

Тези наукових доповідей:

18. Бурячок В.Л., **Бурячок Л.В.**, Боголій С.М. Порівняльне оцінювання програмних засобів однакового функціонального призначення. «Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення». V-а НТК ВІТІ НТУУ "КПІ" МО України, 20–21.10.2010 р.. Доповіді та тези доповідей. – К.: ВІТІ НТУУ "КПІ", 2010. – С. 75–76.

19. **Бурячок Л.В.** Класифікація соціотехнічних систем за методом кластерізації кількісних даних. «Проблеми кібербезпеки інфрормаційно-телекомунікаційних систем». НТК Київського національного університету імені Тараса Шевченка, 10-11.03.2016. Збірник матеріалів доповідей та тез. – К.: НУ ТГШ, 2016. – С. 24–25.

20. Бурячок В.Л., **Бурячок Л.В.,** Гадицький М.Г. Цифрова стратегія безпеки критично важливих об'єктів державної інформаційно-комунікаційної інфраструктури. Матеріали Регіональної конференції МСЕ для країн СНД та Грузії «Перспективи надання послуг на основі мереж пост-NGN, 4G и 5G. Організаційні і технічні рішення щодо їх побудови та захисту», ДУТ, 7-9.06.2017. – К.: ДУТ, 2017. – С. 105–108 (електронний ресурс)

21. **Кузьменко Л.В.,** Бурячок В.Л. Тенденції розвитку та особливості забезпечення безпеки сучасних IOT-пристроїв. І міжнародна науково-практична конференція «Проблеми кібербезпеки інфрормаційно-телекомунікаційних систем». Збірник матеріалів НПК Київського національного університету імені Тараса Шевченка, 05-06.04.2018. – К.: НУ ТГШ, 2018. – С. 264–268

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

АС	–	автоматизована система
АСУ	–	автоматизована система управління
АРМ	–	автоматизоване робоче місце
БД/БЗ	–	база даних / база знань
ЕОМ	–	електронна обчислювана машина
ІР	–	інформаційний ресурс
ІС	–	інформаційна система
ІТП	–	інформаційно-технологічний процес
ІТС	–	інформаційно-телекомунікаційна система
КМ	–	комп’ютерна мережа
КС	–	комп’ютерна система
ЗПЗ	–	загальне програмне забезпечення
МАІ	–	метод аналізу ієрархій
НДР	–	науково-дослідна робота
НСД	–	несанкціонований доступ
ОІД	–	об’єкт інформаційної діяльності
ОКІ	–	об’єкт критичної інфраструктури
ОС	–	операціна система
ПЗ	–	програмне забезпечення
ПАЗ	–	програмно-апаратний засіб
ПЗРА	–	програмний засіб реалізації атак
СЕДО	–	система електронного документообігу
СПЗ	–	спеціальне програмне забезпечення
СУБД	–	система управління базами даних
ТТХ	–	тактико-технічні характеристики

ВСТУП

Обґрунтування вибору теми дослідження. Ключовою тенденцією розвитку сучасної світової цивілізації є застосування цифрових технологій. Підтвердженням цьому слугує цифрова трансформація промисловості, логістики, системи продаж, сервісу тощо. Експерти фінансового ринку прогнозують, що дохід економіки від проявів цифрової трансформації сягне до 2025 року біля 30 трлн. USD. Разом з цим експерти стверджують, що такий стан справ вимагатиме суттєвої трансформації, власне, й інформаційно-телекомунікаційної індустрії. Більшою мірою це стосуватиметься автоматизованих систем (АС), включених в контури управління інформаційними та/або технологічними процесами (ІТП) об'єктів критичної інфраструктури (ОКІ), а також інформаційними ресурсами (ІР), які в умовах кібернетичних втручань і загроз забезпечують необхідні послуги та/або сервіси ОКІ. Негативними наслідками такої трансформації може бути виникнення нових ризиків для безпеки ІТП та ІР, що, як результат, й генерує потребу в побудові та впровадженні сучасних інформаційних технологій (ІТ) для створення перспективних гарантоздатних (ПГ) автоматизованих систем управління (АСУ), захищених від впливу антропогенних і техногенних загроз.

Незважаючи на нормативно-правову урегульованість питань щодо створення інформаційно-телекомунікаційних систем (ІТС) для потреб ОКІ та оцінювання стану їх захищеності від впливу шкідливих програм, фальшивого ПЗ і злоякісних шифруючих кодів, на сьогодні ще й досі спостерігається:

дублювання інформаційних потоків та накопичення ОКІ надлишкового навантаження на засоби зберігання інформації;

технологічна нерівність ОКІ у сфері інформаційних, телекомунікаційних та інших високих технологій;

недостатність глибини наукових досліджень щодо створення для потреб ОКІ новітніх захищених АСУ, а також подекуди повна відсутність рішень щодо специфіки їх функціонування; недосконалість методів, моделей і методик вирішення відповідних завдань.

Саме тому ***наукова задача***, яка полягає в розробленні теоретичних і прикладних засад побудови інформаційної технології для створення перспективних гарантоздатних автоматизованих систем управління об'єктами критичної інфраструктури, а також визначення впливу на процеси функціонування таких систем антропогенних і техногенних втручань та загроз ***є актуальною і потребує розв'язку***.

Дослідженню проблеми побудови перспективних гарантоздатних АСУ та визначення впливу на процеси функціонування таких систем антропогенних і

техногенних втручань та загроз присвячено роботи П.О. Балашова, М.М. Будько, В.Л. Бурячка, В.Б. Дудикевича, Н.Ф. Казакової, О.В.Копійка, Д.В.Ланде, М.І.Паламаря, Д.В. Стефанишина, І.Ю.Субача, О.М.Трофимчука, В.С.Харченка, W.Jansen, D.Catteddu, K.Stoddart та багатьох інших. За результатами їх досліджень встановлено, що особливістю вирішення зазначеного завдання є недостатність статистичної інформації, а також наявність невизначеностей та протиріч, викликаних:

1) відносно високим рівнем розвитку засобів автоматизації та низьким науково-методичним рівнем досліджень властивостей якості АСУ ОКІ;

2) рівнем відмовостійкості, закладеним у конструкцію АСУ ОКІ та її необхідним рівнем;

3) зростанням витрат на розробку, виробництво та експлуатацію АСУ ОКІ і реальними економічними можливостями замовника;

4) необхідним рівнем продуктивності та обмеженими можливостями промислової бази з виробництва якісної елементної бази і комплектуючих виробів, тощо.

Зв'язок роботи з науковими програмами, планами, темами.

Дисертаційна робота та отримані результати пов'язані з вирішенням науково-технічних задач, сформульованих в Стратегії національної безпеки України (Указ Президента України № 287/2015 від 26.05.2015 р.), «Порядку формування переліку ІТС об'єктів критичної інфраструктури держави» (Постанова КМ України № 518 від 19.06.2019 р.), «Основних наукових напрямах та найважливіших проблемах фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук НАН України на 2014–2018 роки». Частину завдань дисертаційної роботи автором вирішено в рамках таких науково-дослідних робіт, як: «Розробка інформаційного інструментарію еколого-економічного прогнозування надзвичайних ситуацій техногенного та природного характеру з метою захисту об'єктів критичної інфраструктури» (№ д.р. 0116U000797), «Базис-Наука» (№ д.р. 0119U000042дс) та «Розробка науково-технічних пропозицій з організації віддаленого управління станціями оптико-електронних спостережень типу 1 та типу 2» (№ д.р. 0120U105420), які у 2020 році виконано відповідно в ІТГІП НАН України, ІПММС НАН України і Національному центрі управління та випробувань космічних засобів України.

Мета і завдання дослідження. Метою дисертаційної роботи є побудова інформаційної технології для створення перспективних гарантоздатних автоматизованих систем управління об'єктами критичної інфраструктури України, здатних гарантовано надавати абонентам необхідні послуги та/або сервіси, яким в заданих режимах і умовах застосування з урахуванням стану захищеності таких систем від загроз порушення цілісності, конфіденційності та доступності (ЦКД) можливо виправдано довіряти.

Для досягнення поставленої мети в роботі необхідно розв'язати такі **завдання**:

1) дослідити можливі загрози та сформувати їх актуальну множину, а також множину уразливостей безпеці функціонування АСУ ОКІ;

2) розробити часткову модель загроз безпеці ПГ АСУ ОКІ;

3) розробити метод визначення впливу загроз на процеси функціонування ПГ АСУ ОКІ;

4) вдосконалити метод формування типового варіанту побудови ПГ АСУ ОКІ.

Зважаючи на таке ***об'єктом дослідження*** в роботі є процеси створення перспективних гарантоздатних АСУ та процеси функціонування таких систем в умовах впливу антропогенних і техногенних втручань та загроз. ***Предметом дослідження*** – інформаційна технолоія, спрямована на формування типового варіанту побудови ПГ АСУ, а також визначення впливу загроз порушення цілісності, конфіденційності та доступності (ЦКД) на процеси функціонування такої системи.

Методи дослідження. При вирішенні поставлених задач в дисертаційній роботі було використано класичні та похідні критерії вибору рішень в умовах невизначеності, «евристичні» (експертні) методи оцінювання – метод Дельфи, метод аналізу ієрархій (MAI) та метод парних порівнянь, а також метод морфологічних карт, методи лінійного програмування, методи функціонально-вартісного (ФВА) та кластерного аналізу тощо.

Наукова новизна отриманих результатів полягає в подальшому розвитку теоретичних і практичних методів та моделей побудови і визначення впливу загроз на процеси функціонування перспективних гарантоздатних АС переробки інформації та управління. Новими результатами, отриманими в дисертаційній роботі, є:

1) вперше розроблений ***метод визначення впливу загроз на процеси функціонування перспективних гарантоздатних АСУ ОКІ***, впровадження якого шляхом реалізації *семантичної моделі протиборства системи захисту ПГ АСУ ОКІ з атакуючою стороною, алгоритму детектування та відновлення даних та моделі оцінки стану захищеності такої системи від загроз порушення ЦКД* **дозволяє**, на відміну від існуючих, відслідкувати вплив шкідливих програм, фальшивого ПЗ і злоякісних шифруючих кодів на ІТП в АСУ ОКІ, відшукати вразливості та/або істинні значення ключів, застосованих для шифрування даних в ПГ АСУ ОКІ, оцінити стан захищеності сформованого прототипу варіанту побудови ПГ АСУ ОКІ від впливу кібератак та убезпечити АСУ ОКІ від НСД до її ресурсів та інформації, що в ній циркулює;

2) удосконалений ***метод формування типового варіанту побудови перспективної гарантоздатної АСУ,*** впровадження якого *за рахунок розробки*

процедури вибору прототипу топології мережевої інфраструктури, процедури вибору типового АРМ раціональної конфігурації, процедури раціонального вибору ПЗ ПР та процедури вибору типового варіанту побудови ПГ АСУ ОКІ **дозволяє,** на відміну від існуючих, організувати доступ до мережі та надання обчислювальних ресурсів і послуг абонентам для спільного використання ними власних і зовнішніх ІР, забезпечити доступ користувачам до таких ІР, керування їх обміном, передачею та машинною переробкою, автоматизувати процеси пошуку і збору інформації у зовнішніх і внутрішніх джерелах, її реєстрації, трансформації та функціональної обробки, а також процеси захисту ІР в АСУ від кібернетичних загроз.

Практичне значення отриманих наукових результатів полягає в тому, що вони за рахунок реалізації методу формування типового варіанту побудови такої системи та методу визначення впливу загроз на процеси її функціонування **дозволили розробити прикладні засади побудови інформаційної технології для створення ПГ АСУ ОКІ**, впровадження якої на відміну від існуючих забезпечує гарантоване надання абонентам необхідних послуг та/або сервісів, яким в заданих режимах і умовах застосування з урахуванням стану захищеності таких систем від загроз порушення ЦКД можливо виправдано довіряти. Разом з цим впровадження ІТ для створення ПГ АСУ ОКІ на прикладі НЕК «Укренерго» сприяє:

по-перше, підвищенню ефективності дій осіб, відповідальних за забезпечення безпеки ПГ АСУ ОКІ (за рахунок оперативного визначення найбільш значимих загроз та своєчасного реагування на стан захищеності АСУ від загроз порушення ЦКД) приблизно на 12%;

по-друге, скороченню часу на прийняття виважених управлінських рішень щодо побудови ПГ АСУ ОКІ з відповідним ПАЗ та їх впровадження приблизно на 18 - 20%.

Результати дисертаційного дослідження впроваджено в:

Інституті проблем математичних машин і систем НАН України при дослідженні проблеми побудови різнорідних інформаційних систем ситуаційних центрів сектору безпеки і оборони та обміну даними між ними (Акт впровадження від 03.12.2020 р.);

Національному центрі управління та випробувань космічних засобів для оцінювання стійкості криптосистем та пошуку вразливостей або істинних значень ключів, застосованих при зловмисному шифруванні даних (Акт впровадження від 17.12.2020 р.);

НЕК «УкрЕнерго» під час виконання робіт зі створення та розгортання ІТС для потреб її структурних підрозділів, а також при налаштуванні SIEM систем, спрямованих на вирішення завдань захисту таких ІТС від сучасних кіберзагроз (Акт впровадження від 04.01.2021);

Азербайджанскому Технічному Університеті при підготовці магістрантів спеціальності 050627 «Інженерія електроніки, телекомунікації та радіотехніки» за спеціалізацією «Інформаційна безпека телекомунікаційних систем» (Акт впровадження від 05.01.2021).

Особистий внесок здобувача. Основні положення і результати дисертаційної роботи, що виносяться на захист, отримані автором самостійно. У роботах, написаних у співавторстві, автору належать: [1] – результати експерименту щодо навантаження вбудованих апаратних платформ для IoT рішень при розгортання невеликих комерційних та наукових бездротових мереж; [2] – технологія захисту освітніх матеріалів та іншої інформації обмеженого доступу, а також ІТ-інфраструктури ЗВО від випадкових або спрямованих атак та шкідливого ПЗ; [3] – обґрунтування підходу до побудови та вибору раціональної топології комп'ютерних мереж сучасних АСУ ЗС України, що сприятиме підвищенню оперативності, стійкості, скритності, безперервності й ефективності управління військами; [4, 18] – алгоритм порівняльного оцінювання ПЗ однакового функціонального призначення (на прикладі СУБД та СЕДО), що спрямовані на розв'язання нагальних завдань інформаційної діяльності; [5] – обґрунтування набору показників, які можуть бути використані для оцінювання якості та подальшого порівняльного аналізу ПЗ сучасних АС; [6] – алгоритм обґрунтованого вибору серед множини існуючих АРМ раціональної конфігурації; [7, 13] – алгоритм обґрунтованого вибору серед множини існуючих раціональної системи електронного документообігу; [8] – обґрунтування необхідності створення системи комплексної оцінки стану захисту інформації в розподілених корпоративних мережах; [9] – обґрунтування необхідності захисту критично-важливих сегментів та об'єктів економіки держав світу від загроз антропогенного і техногенного характеру; [10] – обґрунтування раціонального набору параметрів і функцій ПЗ спеціального призначення, спрямованих на розв'язання завдань інформаційної діяльності; [11] – алгоритм порівняльного аналізу автоматизованих ІС на підставі заздалегідь обраного набору ознак (властивостей) та комплексного показника якості системи; [12] – процедура формування системи детектування шкідливого ПЗ на базі застосування методів виділення значимих ознак в ІТ системах; [14, 19] – застосування методу кластеризації кількісних даних для вирішення задачі розпаралелювання операцій пошуку істинних значень застосованих ключів та визначенні місця соціальної інженерії в ході проведення розвідки ІТС; [15] – шляхи управління процедурою інвестування в ІТ з урахуванням їх багатофакторності та захисту інформації обмеженого доступу, а також ІТ-інфраструктури від випадкових або спрямованих атак та шкідливого ПЗ; [16] – технологія забезпечення інформаційної і кібербезпеки ЗВО України від стороннього

кібернетичного впливу та захисту інформації обмеженого доступу, а також ІТ-інфраструктури ЗВО від випадкових або спрямованих атак та шкідливого ПЗ; [17] – технологія визначення наявності бездротових точок доступу та оцінки негативних наслідків витоку персональних даних під час їх обробки в АС; [20] – процедура виявлення та організації кіберзахисту об'єктів критичної інфраструктури України від впливу найбільш небезпечних векторів атак, зокрема від впливу шкідливого ПЗ; [21] – технологія захисту середовища IoT від випадкових або спрямованих атак та шкідливого ПЗ на етапах розробки та експлуатації.

Апробація результатів дисертації. Основні положення і результати досліджень доповідалися та обговорювалися на наукових конференціях та семінарах, серед яких: V-а НТК Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення» (м. Київ, ВІТІ НТУУ "КПІ" МО України, 2010), НТК «Проблеми кібербезпеки інфрормаційно-телекомунікаційних систем» (м. Київ, КНУ імені Т.Г. Шевченка, 2016 та 2018 р.р.), Регіональній конференції МСЕ для країн СНД та Грузії «Перспективи надання послуг на основі мереж пост-NGN, 4G и 5G. Організаційні і технічні рішення щодо їх побудови та захисту» ДУТ (м. Київ, ДУТ, 2017), VIII International conferece of students, PHD-students and young scientists «Engineer of XXI Century» (University of Belsko-Biala, Poland, 2018), X International conferece of students, PHD- students and young scientists «Engineer of XXI Century» (University of Belsko-Biala, Poland, 2020).

Публікації. Основні положення дисертаційної роботи опубліковано у 21 науковій праці, з яких: 2 публікації – розділ колективної монографії [1] та [2]; 12 – у вітчизняних фахових наукових виданнях, які входять до міжнародних наукометричних баз даних (*Index Copernicus, CORE, BASE, ResearchBib, PKP*, тощо) [3–14]; 3 – у міжнародних рецензованих видання-х, що входять до баз даних *Scopus* та *Web of Science* [15–17] та 4 тез доповідей [18–21]. Без співавторів опубліковано 1 наукову статтю і 1 тези доповідей.

Обсяг і структура дисертації. Дисертація складається з анотації, змісту, переліку умовних позначень, вступу, чотирьох розділів, загальних висновків, списків використаних джерел (в кінці кожного розділу основної частини дисертації) і 148 сторінок основного тексту, 48 рисунків, 38 таблиць. Список використаних джерел за чотирма розділами містить 149 унікальних найменувань і займає 12 сторінок. Загальний обсяг дисертаційної роботи – 181 сторінка. Кількість сторінок додатку – 35.

Розділ 1
АНАЛІЗ СТАНУ ПРОБЛЕМИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ТА ЗАБЕЗПЕЧЕННЯ ГАРАНТОЗДАТНОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВПЛИВУ ЗАГРОЗ І УРАЗЛИВОСТЕЙ

Людству (за оцінками) біля 60 тисяч років. За цей час змінилося понад 1800 поколінь, з яких лише два покоління володіли атомною енергією, телебаченням, авіацією, лазерами, антибіотиками й тільки одному з них в цей період властивою виявилась інформаційна глобалізація. Її виникненню у XVIII – XIX ст. сприяли:

по-перше, чотири світові індустріальні та одна інформаційна революції;

по-друге, два простих, але надзвичайно змістовних закони, сформульовані Гордоном Муром (одним із засновників корпорації Інтел), який фактично пояснює формування на рубежі тисячоліть простору інформаційного та Робертом Меткалфом (винахідником найпоширенішої технології комп'ютерної мережі Інтернет), який констатує, що домінування в життєдіяльності людства ІТ систем та мереж різного призначення обумовило появу та формування простору кібернетичного.

Це, в свою чергу, обумовило формування сучасного інформаційного суспільства, призвело до синтезу двох інформаційно-комунікаційних технологій – інформаційної та телекомунікаційної й, як наслідок, дозволило виокремитись як деяким глобальним субстанціям – спочатку простору інформаційному, а згодом й простору кібернетичному. Але, разом з цим, питання щодо міждержавного паритету та взаємовідносин в інформаційному і кіберпросторах, на відміну від таких просторів, як наземний, морський, повітряний та космічний, залишило відкритими, тобто такими, що потребують подальшого розв'язку [1, 2].

Такий стан справ пояснюється передусім безпрецедентним впливом на сучасне суспільство, інформаційний та кіберпростори низки інформаційних та кібероперацій, які для переважної більшості держав нині:

1) стали невід'ємною частиною їх внутрішньої і зовнішньої політики;

2) відіграють суттєву роль в їх економічному і соціальному розвитку;

3) свідчать про їх вступ до якісно нової фази взаємовідносин – інформаційного та кіберпротиборства [3].

Наряду із зростанням обсягів інформації, до яких отримали доступ пересічні громадяни, та їх переходом в хмару, винайденням потужних комп'ютерів та вбудованих мікроконтролерів, що сприяло розвитку промисловості, а також прийняттям рішень у режимі реального часу все це спонукає країни світу не тільки до глобальної інтелектуалізації та отриманню ними певних переваг, але й сприяє виникненню низки проблем – передусім безпекового характеру, роблячи при цьому інфраструктуру цих країн більш вразливою до загроз антропогенного і техногенного характеру та

природних катаклізмів. Підтвердженням цьому може бути цифрова трансформація всіх сфер життєдіяльності суспільства й передусім промисловості, реалізації якої в останнім часом, починаючи з 60-х років минулого століття сприяла поява мейнфреймів та баз даних, настільних систем і персональних комп'ютерів, спеціального програмного забезпечення для роботи компаній, Інтернету та електронних систем комунікації, мобільного широкосмугового доступу, соціальних мереж, big data та IOT, безпілотних літальних апаратів, робототехніки, штучного інтелекту тощо (рис.1.1).

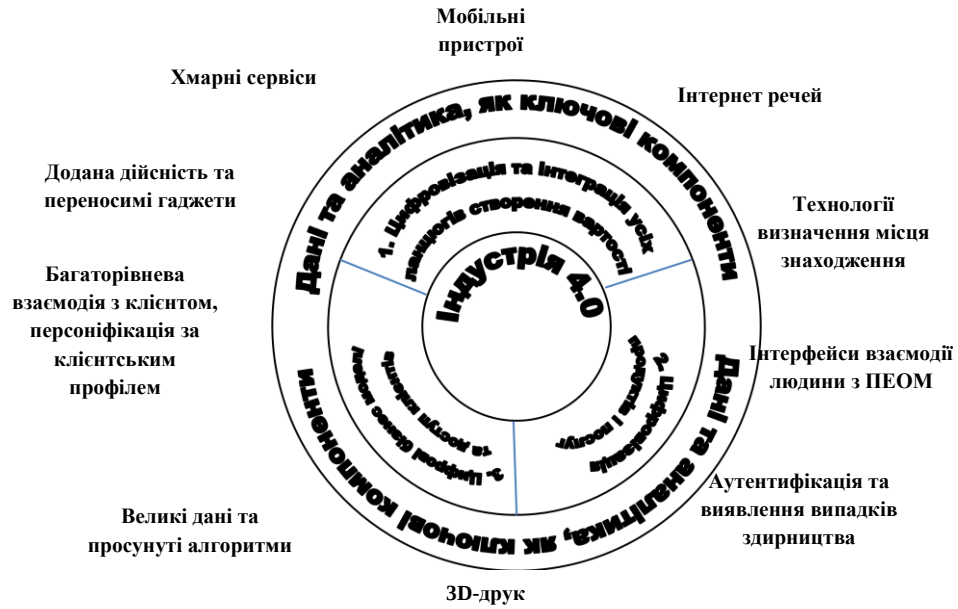


Рис.1.1. Наскрізні цифрові технології

Наслідком таких інновацій стало те, що границі поміж індустріями почали поступово зникати, а зміни бізнес-ландшафту почали регулярно спостерігатися через кожні 3-5 років. Прикладом такому є процеси, які до цього часу:

по-перше, за рахунок розвитку засобів комунікації сприяли:

становленню соціальних мереж;

виникненню технології електронного поштового обміну;

розвитку технологій обміну миттєвими повідомленнями;

розвитку систем відео зв'язку та Інтернет телефонії;

по-друге, за рахунок розвитку інформатизації та забезпечення автоматизації критичних виробничих процесів призвели до:

створення локальних (корпоративних) обчислювальних мереж;

формування нових платформ для роботи користувачів;

удосконалення технологій доступу до ресурсів;

розвитку СЕДО, систем та технологій управління;

створення систем планування ресурсів підприємств;

розвитку послуг Інтернет-банкінгу, електронної комерції тощо.

Як результат, експерти фінансового ринку прогнозують, що до 2025 року до цифрових технологій, які будуть найбільш перспективними для міжнародного бізнесу, приєднається надзвичайно багато нових напрямів (таблиця 1.1), а дохід світової

Таблиця 1.1

Перспективні напрями розвитку цифрових технологій у країнах світу

Європейський союз	США	Китай	Україна
Нові адаптивні і розумні виробничі процеси; Цифрове, віртуальне і рефлексорне виробництво; Мобільні підприємства, спроможні кооперуватися (мережеве виробництво та динамічні виробничі ланцюги); Виробничий «людиноцентризм»; Виробництво, орієнтоване на споживача	Вимірювання і контроль процесів, застосування сенсорів; Сучасні дизайн матеріалів, технології синтезу та обробки; Цифровізація і візуалізація сталого (раціонального) виробництва; Впровадження промислових нанотехнологій, біотехнологій та біоінформатики, робототехніки; Виробництво гнучкої електроніки, впровадження технологій 3D-друку; Розробка і впровадження обладнання для тестування (контролю якості)	ІКТ-індустрія нового покоління; Біоінженерія; Високопродуктивні технології та обладнання; Сучасні матеріали; Розумні технології	ІКТ-індустрія нового покоління (передусім в сфері програмної інженерії); Нові композиційні матеріали із заданими властивостями; Промислові нано- та біотехнології (біомедицина, фармацевтика та аграрний сектор); Створення розумних виробничих систем; Нові розробки для розвит-ку космічної галузі

економіки від проявів цифрової трансформації до 2025 року може сягнути до 30 трлн. USD (рис.1.2).

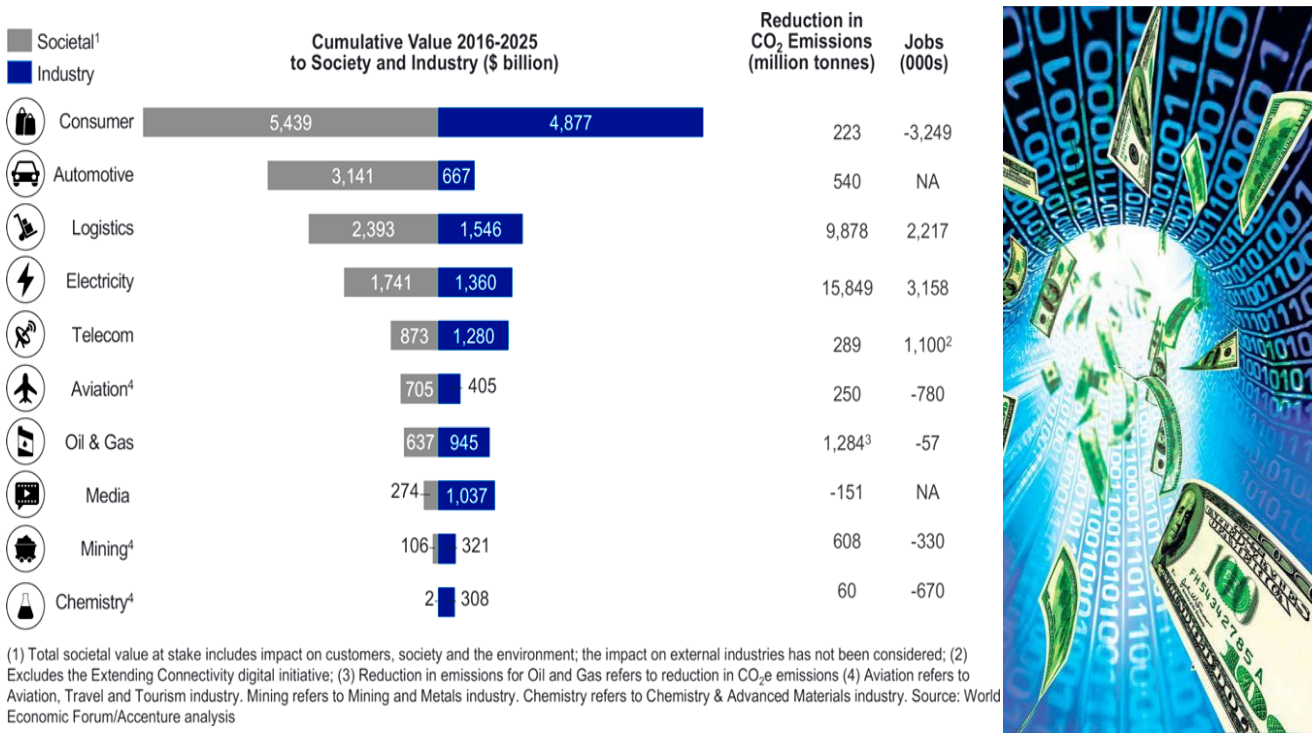


Рис.1.2. Прогноз доходу світової економіки від проявів цифрової трансформації

Разом з тим, впровадження нових технологій створює середовище як для появи нових загроз і ризиків, так й передумови щодо захисту від них. Більшою мірою це стосується об’єктів критичної інфраструктури країн світу та відповідного інформаційного ресурсу (рис.1.3). [4, 5].

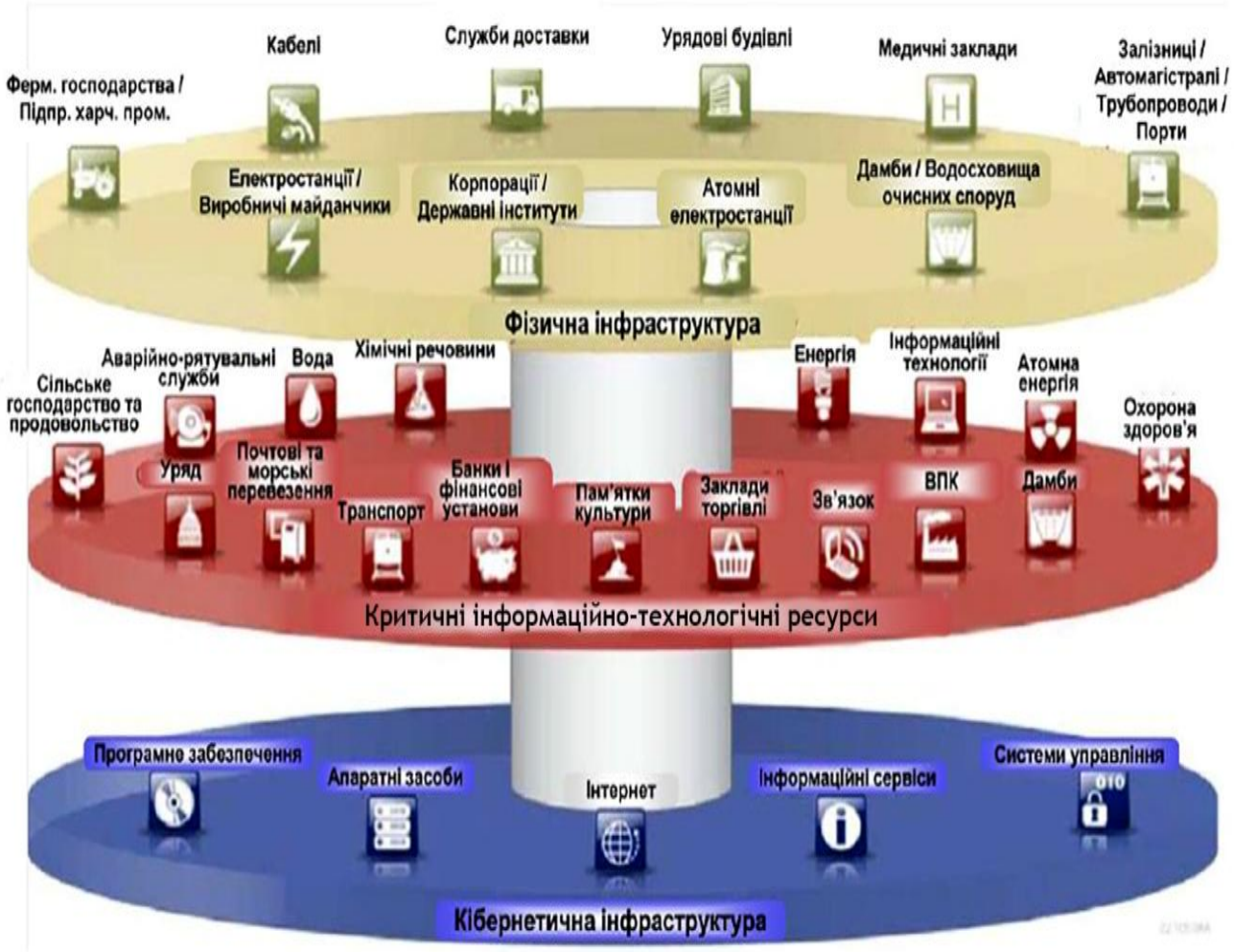


Рис.1.3. Об’єкти критичної інфраструктури країн світу.

Термін ОКІ не має усталеного тлумачення й тому кожна держава привносить в нього свій зміст і свою специфіку. Наприклад, у США під ОКІ розуміють комплекс фізичних та віртуальних активів, систем і мереж, що мають життєво важливе значення для держави, руйнування або недієздатність яких, в тому числі і окремих їх елементів, матиме згубні наслідки для національної безпеки, економіки, безпеки і здоров’я населення, чи матиме будь-яку комбінацію з перелічених наслідків (USA Patriot Act of 2001). В ЄС до ОКІ відносять активи, системи або їх частини, що розташовані в державах-членах Європейського Союзу, які мають важливе значення для основних життєво важливих соціальних функцій, здоров’я, безпеки, еко-номічного або соціального благополуччя людей, а також порушення або руйнування яких матиме значний вплив на спроможність держави виконувати свої функції (COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European criti-cal infrastructures and the assessment of the need to improve their protection).

Перелік ОКІ економічно розвинених країн світу подано в таблиці 1.2.

Таблиця 1.2

Перелік критично важливих секторів світової економіки

№ з/п	Сектор	Країна				
		США	Швейцарія	Велико-британія	Японія	Канада
1.	Інформаційно-комунікаційний	+	+	+	+	+
2.	Аварійно-рятувальних служб	+	-	+	-	-
3.	Енергетичний	+	+	+	-	+
4.	Фінансово-банківський	+	+	+	+	+
5.	Продовольчий (та сільське господарство)	+ (+)	+	+	-	+
6.	Державного управління	+	+	+	+	+
7.	Охорони здоров'я	+	+	+	+	+
8.	Транспортний	+	+	+	-	+
9.	Водопостачання	+ (+)	+	+	+	+
10	Оборонний	+	-	+	-	-
11	Ядерний	+	-	+	-	-
12	Космічний	-	-	+	-	-
13	Хімічний	+	-	+	-	-
14	Безпеки	-	+	-	-	+
15	Промисловий	+	-	-	-	+
16	Повітропровідний	-	-	-	+	-
17	Залізничний	-	-	-	+	-

Поняття критичної інфраструктури розкрито і в нормативно-правових актах України: Стратегії національної безпеки України (Указ Президента України від 26.05.2015 №287/2015); Стратегії кібербезпеки України (Указ Президента України від 15.03.2016 №96 / 2016); Законі України «Про основні засади забезпечення кібербезпеки України» (05.10.2017, №2163-VII); Постановах КМУ від 19.06.2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» та від 09.10.2020 р. № 943 щодо «Деяких питань об'єктів критичної інформаційної інфраструктури». Так, наприклад, в Законі України «Про основні засади забезпечення кібербезпеки України» [48] поняттю ОКІ дано таке визначення: «критично важливі об'єкти інфраструктури (далі - об'єкти критичної інфраструктури) - підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього

природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей». Виходячи з цього до сімейства ОКІ в Україні відносять хімічну промисловість, електроенергетику, газотранспортну систему, автомобільні магістралі, морські порти, атомну енергетику, систему телекомунікацій. У 2015 році до ОКІ в Україні були віднесені заклади медицини та освіти, а також фінансовий сектор. В даний час до таких об'єктів прийнято відносити кіберінфраструктуру, що стала ключовим елементом функціонування пере важної більшості країн світу, високо технологічні підприємства і підприємства оборонно-промислового комплексу, центральні органи влади і т.п., а також критичне важливе інформаційне середовище (рис.1.4).

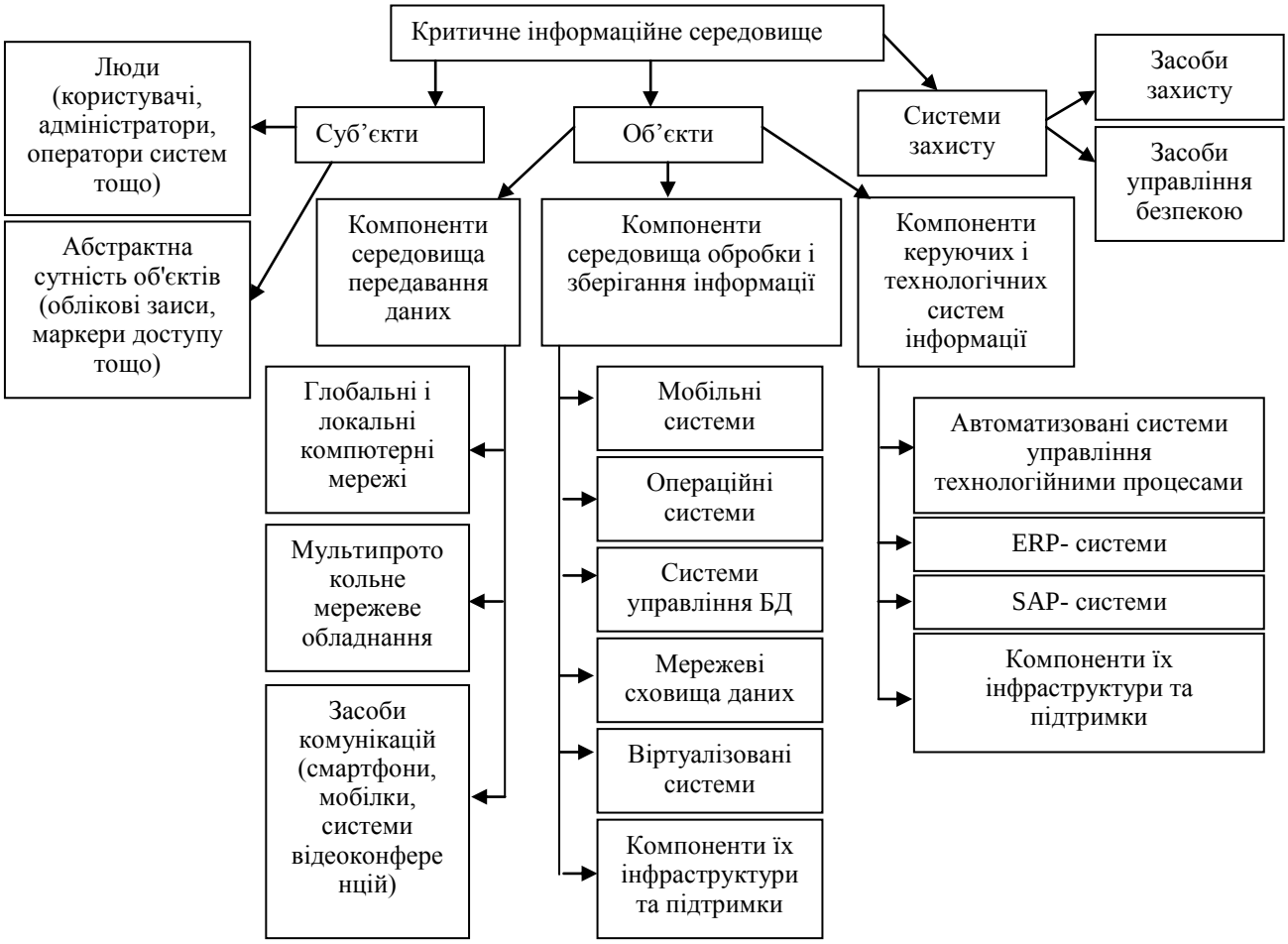


Рис.1.4. Критично-важливе інформаційне середовище

Враховуючи таке Постановою КМ України від 9 жовтня 2020 р. № 943 щодо «Деяких питань об'єктів критичної інформаційної інфраструктури» [49] затверджено «Порядок формування переліку об'єктів критичної інформаційної інфраструктури» та «Порядок внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування». Постановою КМ України від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» [50] визначено перелік базових вимог із забезпечення кіберзахисту об'єктів критичної

інфраструктури. Серед них найбільш важливими визначено процедури:

формування на ОКІ загальної політики інформаційної безпеки;

управління доступом користувачів та адміністраторів до об'єктів захисту об'єкта критичної інформаційної інфраструктури ОКІ;

ідентифікації та автентифікації користувачів та адміністраторів об'єкта критичної інформаційної інфраструктури ОКІ;

реєстрації подій компонентами об'єкта критичної інформаційної інфраструктури ОКІ та їх періодичний аудит;

забезпечення мережевого захисту компонентів та інформаційних ресурсів об'єкта критичної інформаційної інфраструктури ОКІ;

забезпечення доступності та відмовостійкості компонентів та IP об'єкта критичної інформаційної інфраструктури ОКІ;

визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації на об'єкті критичної інформаційної інфраструктури ОКІ;

визначення умов використання програмного та апаратного забезпечення об'єкта критичної інформаційної інфраструктури ОКІ;

визначення умов розміщення компонентів об'єкта критичної інформаційної інфраструктури ОКІ.

Головну роль в процесах функціонування ОКІ країн світу останнім часом відіграє мережа Internet. Завдяки винаходу і впровадженню перспективних інформаційно-комунікаційних технологій та надпотужних ЕОМ це дозволило [5]:

по-перше, забезпечити доступ до світових обсягів інформації практично всього населення планети Земля;

по-друге, визнати сучасні ІТ системи та мережі електронною артерією всього людства.

Саме це створює передумови того, що ключові сегменти критичної інфраструктури країн світу все частіше стають об’єктами деструктивних антропогенно-техногенних і природніх впливів. Статистику результатів нападів на ОКІ в світі та можливі сценарії кібернетичних впливів подано відповідно на рис.1.5 та в таблиці 1.3.

Рис.1.5. Статистика результатів нападів на ОКІ в світі

Таблиця 1.3

Малоймовірні та найбільш можливі сценарії впливу на ОКІ

Об'єкти критичної інфраструктури	Сценарій кібервпливу		Примітка
	Малоймовірний	Найбільш можливий	
ЕЛЕКТРИКА	Фізичне руйнування електростанцій або ліній зв'язку може призвести до відключення електрики на невизначений період	Атаки на системи керуваннння через бездротові, модемні та Інтернет зєднання може стати причиною локального відключення електрики	Підключення до Інтернет не означає, що існує можливість доступу до АСУ електричних компаній
ТРАНСПОРТ	Використання на потягах пального, що містить небезпечні речовини може призвести до отруєння навколишнього середовища	Атакуючий може через Інтернет підключитися до АСУ залізничним рухом й викликати зіткнення електропотягів, спрчмувавши їх на один шлях	З появою кіберзагроз захист від них став серйозною проблемою на транспорті
ВОДНІ РЕСУРСИ	Нині зявилась загроза здійсннння атак на системи управлінння водними ресурсами через Інтернет	Вода може бути фізично заражена хімічними речовинами. Але чисельні перевірки її складу зводять цей ризик зараження до мінімуму	Більшу частину грошей, які виділяються на захист водних ресурсів доцільно зосередити саме на їх фізичному захисті
ЕНЕРГЕТИКА	Фізичне руйнування нафтопереробних заводів і трубопроводів може призвести до тимчасового відключення джерел енергії або катастрофи навколишнього середовища	Виведення з ладу мережі Інтернет, використовуваної в системі торгівлі нафтою (гасом), може зупинити процеси купівлі/продажу й призвести до дефіциту джерел енергії	Будь-яке втручання до Інтернет може породити проблеми в енергетиці. Приклад такому – виведення з ладу АСУ трансси бірського трубопроводу.
ФІНАНСИ	Фізичне руйнування устаткування або ліній звязку може завдати збитку фінансовим ринкам та зробити їх недоступними протягом тривалого періоду	Кібератаки на мережеве або серверне обладнання, використовуване для проведення фінансових транзакцій може призвести до повного закриття фінансового ринку	Взаємозалежність платіжних і клірингових та інших фінансових систем може призвести до того, що збій в одній з них вплине на всі інші
Інформаційні технології	Уразливості ПЗ використовуються для доступу до критичних систем та атак на елементи їх інфраструктури		Можливості для здійснення кібератак нині необмежені

1.1 Поняття безпеки та шляхи захисту автоматизованих систем управління об'єктами критичної інфраструктури від стороннього кібернетичного впливу

Історія розвитку інформаційного суспільства тісно переплетена зі створенням та впровадженням в усі сфери діяльності людства гарантоздатних (*dependability*) автоматизованих систем (рис.1.6). Нині саме вони є невід'ємним сегментом індустріального Інтернету речей, встановлюються на об'єктах паливно-енергетичного комплексу тощо.

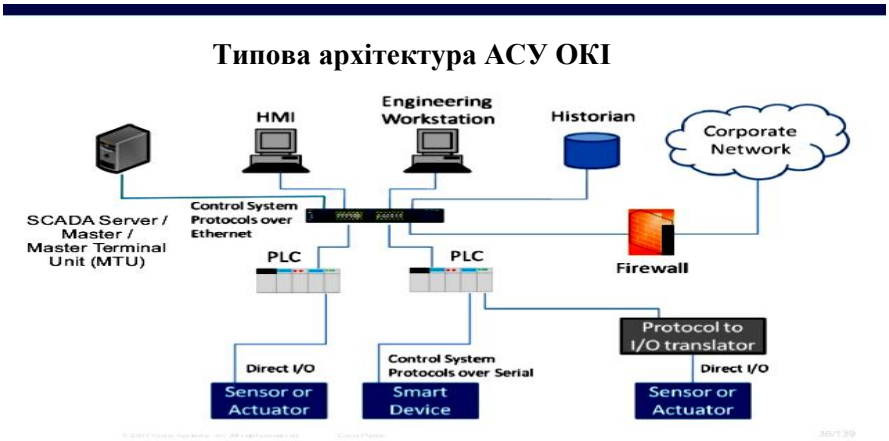


Рис.1.6. Типова автоматизована система управління ОКІ

При цьому під гарантоздатністю АСУ ОКІ слід розуміти їх комплексну властивість, що поєднує аспекти надійності, функціональної та кібернетичної безпеки й забезпечує здатність таких систем надавати необхідні довірчі послуги та виконувати потрібні функції в заданих режимах та умовах застосування [6, 7]. Основними складовими довільної гарантоздатної АСУ ОКІ є (рис.1.7):

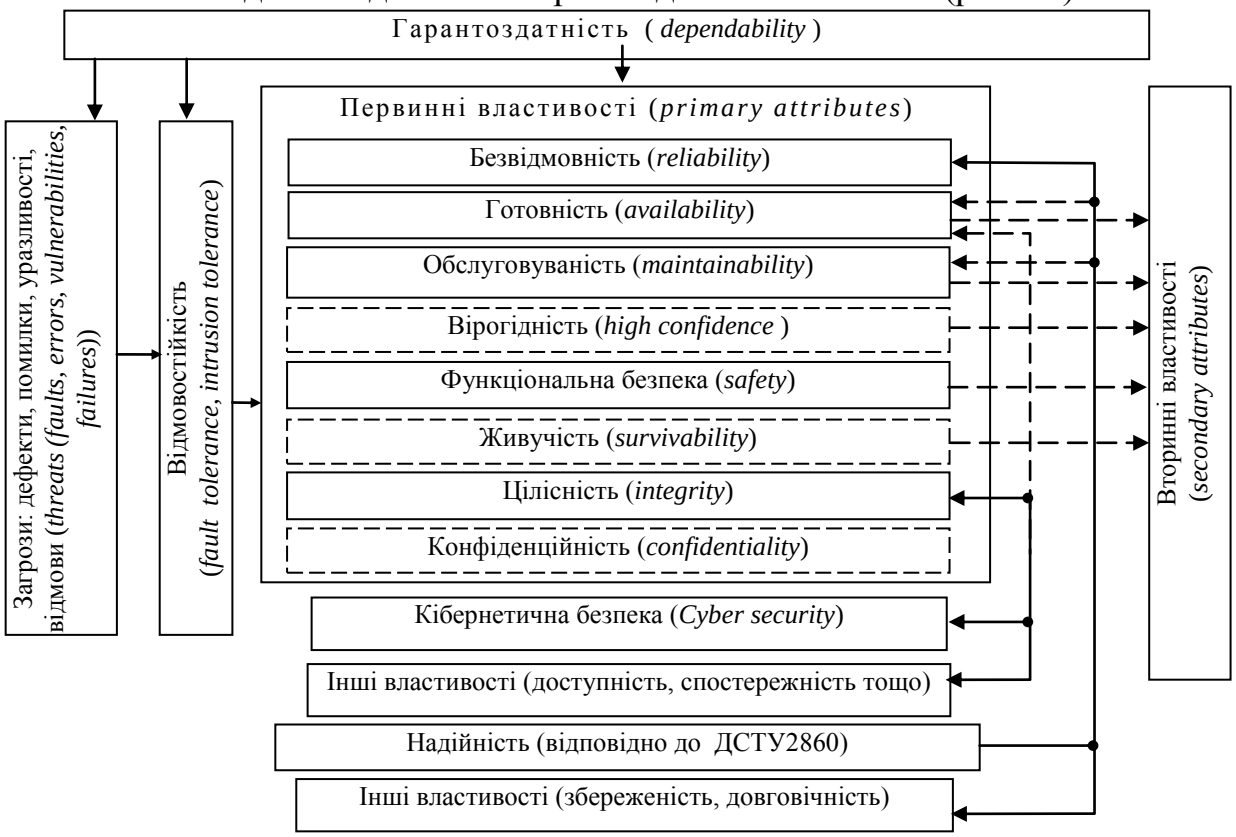


Рис.1.7. Таксономічна схема гарантоздатності АСУ ОКІ

безвідмовність, тобто спроможність безперервно надавати певні послуги впродовж заданого інтервалу;

готовність, тобто спроможність забезпечувати доступність ресурсів для надання необхідних послуг;

обслуговуваність, тобто спроможність пристосовуватися до модифікацій, обслуговування та ремонту;

живучість, тобто спроможність мінімізувати зниження працездатності та зберігати в прийнятних межах обсяг та якість надаваних послуг у разі відмов, обумовлених зовнішніми впливами різної природи;

функціональна безпека, тобто спроможність виключати або мінімізувати шкідливі (включаючи катастрофічні) наслідки у разі відмов для користувачів, інших систем або навколишнього середовища;

кібернетична безпека, тобто спроможність забезпечувати цілісність і конфіденційність інформації та послуг, які АС надаються, а також доступність до них.

Порушенню функціонування АСУ ОКІ можуть сприяти ризики їх безпеці, а також низка атак, викликаних актуальними загрозами та уразливостями. Глобальну карту ризиків безпеці ОКІ, зокрема АСУ такими об’єктами, вперше на загальний розсуд було представлено на Всесвітньому економічному форумі в Давосі у 2007 році [8, 9] (рис.1.8).

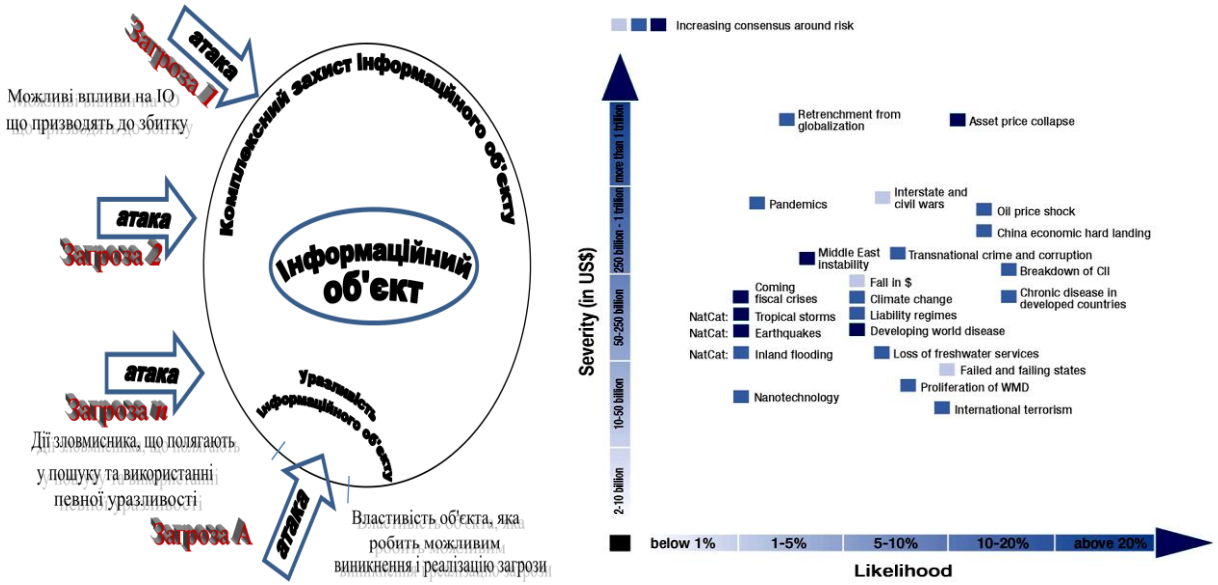


Рис.1.8. Технологія організації атак та глобальна карта ризиків АСУ ОКІ

В ході форуму було відмічено, що найбільш небезпечними серед сучасних ризиків безпеці АСУ ОКІ вважатимуться ті, що при виникненні інцидентів та аварій впливатимуть на фінансові витрати, викликатимуть репутаційні втрати, викликатимуть фінансові втрати від простою потужностей, а також задаватимуть шкоду населенню та оточуючому середовищу.

1.1.1 Загрози функціонуванню програмно-апаратних засобів та їх вплив на стан безпеки АСУ ОКІ

Актуальність питання щодо забезпечення безпеки АСУ ОКІ країн світу обумовлюється тим, що протягом життєвого циклу будь-яка автоматизована система може стикатися з проявами ***халатності*** (підключенням сторонніх ПЕОМ або зовнішніх пристроїв - носіїв інформації, модемів тощо), ***викрадення*** (сировини або готової продукції, ресурсів виробничої лінії або виготовленням необлікованої продукції), ***спланованих атак*** (шпигунство, саботаж тощо), тобто з загрозами, що створюють найвищий рівень небезпеки та характеризуються наявністю намірів, можливості і готовності суб'єкта загрози до нанесення шкоди об'єкту. Результатом цього може стати, наприклад, відхилення в роботі АСУ, що, як результат, обов’язково призведе до збоїв або некоректного проходження певного технологічного процесу.

В США та Канаді до множини загроз, що можуть вплинути на процеси функціонування АСУ ОКІ, наприклад, відносять (рис.1.8) [10 – 14]:

зловмисні дії груп або окремих осіб, таких як терористи і злочинці;

природні небезпеки - урагани, торнадо, землетруси, цунамі, повені тощо;

техногенні надзвичайні ситуації - авіаційні катастрофи, ядерні аварії, пожежі, аварії у системах енергозабезпечення, викиди небезпечних речовин.

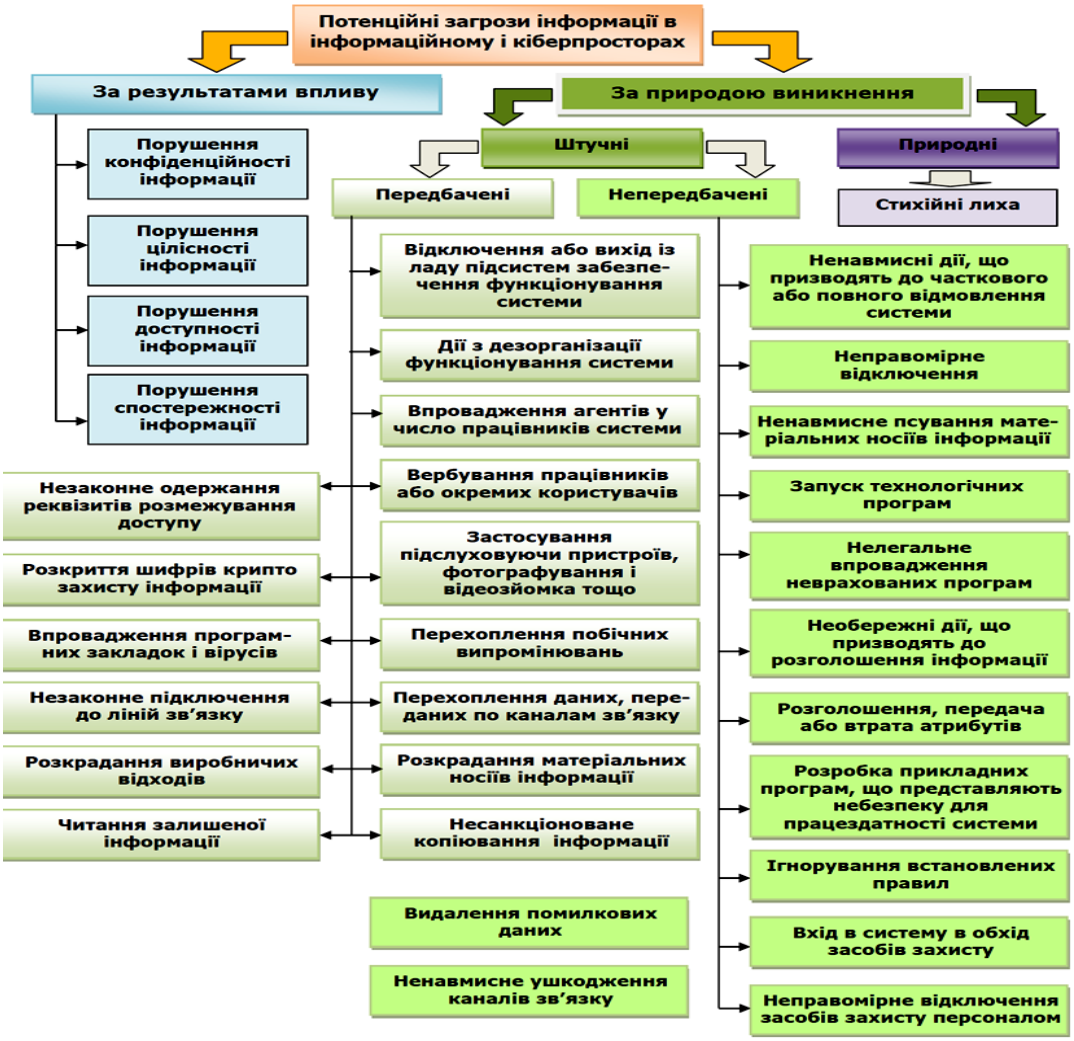


Рис.1.8. Множина штучних і природних загроз АСУ ОКІ

У Німеччині до таких загроз відносять:

небезпечні природні явища (надзвичайні погодні умови, лісові та степові пожежі, сейсмічні явища, епідемії та пандемії, космічні явища);

технічні аварії/людські помилки (відмови систем, аварії та надзвичайні події, недбалість, організаційні помилки);

тероризм, злочинність (терористичні акти, диверсії, злочинні і бойові дії).

При цьому, наприклад, природні загрози можуть бути викликані об'єктивними фізичними процесами й привести до стихійного лиха. Штучні – є наслідком діяльності людини, технічних засобів і систем Вони можуть бути передбачуваними і непередбачуванами, випадковими і навмисними (табл. 1.4), тощо.

Таблиця 1.4

Перелік потенційних загроз ОКІ та причин їх виникнення

Навмисні		**Випадкові**	
Тип	**Причини виникнення**	**Тип**	**Причини виникнення**
Розкрадання носіїв інформації	Прагнення використовувати конфіденційну інформацію у своїх цілях	Несправність апарату-ри, що може ініціювати несанкціоноване зчитування інформації	Недостатня кваліфікація обслуговуючого персоналу, застосування несертифіко-ваних технічних засобів
Застосування програмних пасток		Помилки в програмах обробки інформації	Застосування несертифікованого ПЗ
Використання програм типу “троянський кінь”	Завдання збитків шляхом несанкціонованого доступу в систему	Впровадження комп’ютерного вірусу	Не дотримання обслуговую-чим персоналом вимог безпеки, порушення ним технологічної послідовності роботи із системою
Помилки в програмах обробки інформації	Завдання збитків шляхом внесення програмних за-кладок у процесі розробки програмних систем	Помилкова комутація в мережі ЕОМ	Низька кваліфікація обслуговуючого персоналу
Впровадження комп’ютерного вірусу	Руйнування інформаційної системи з метою завдання збитків	Паразитне електромагнітне випромінювання (ЕМВ)	Недостатнє урахування вимог безпеки на етапі проектування інформаційної системи або її створення
Помилкова комутація в мережі ЕОМ	З метою створення каналу для витоку конфіденційної інформації	Перехресні наведення за рахунок ЕМВ	
Примусове електромагнітне опромінення	Вивід з ладу інформаційної системи з метою завдання збитків	Помилка в роботі оператора	Низька кваліфікація опера-тора, застосування несертифі-кованого ПЗ
Використання акустичних випромінювань	Одержання конфіденційної інформації	Помилки технічного персоналу: перекру-чування схем захисту, помилкова комутація	Недостатня кваліфікація, порушення технології
Копіювання за допомогою візуального й слухового контролю		Помилки користувача	Використання недостатнього захисту
Маскування під користувача, підбор пароля	Несанкціоноване втручання в роботу системи в злочинних цілях		
Помилки програміста: опис і перекручування програмного захисту, розкриття кодів та паролів	З метою добування особистої вигоди або завдання збитків		
Помилки технічного персоналу: опис і перекручування схем захисту, помилкова комутація			

Випадкові загрози можуть бути викликані: помилками проектування ІТС і системи захисту інформації; помилками, збоями та/або відмовами в програмно-апаратних засобах (ПАЗ); помилками персоналу, тощо. Навмисні загрози обумовлені передусім цілеспрямованими діями людей (порушників). За місцем розміщення джерела загроз відносно ОКІ останні розділяються на дистанційні та контактні. До дистанційних відносяться загрози, джерело яких (людина, апаратура, програма тощо) перебуває поза межами контрольованої території. Контактні загрози здійснюються, як правило, в межах контрольованої зони. Результатом дії таких загроз може бути втрата елементів структури об'єкта, порушення зв'язків, програм і функцій об'єкта, втрата здатності об'єкта до розвитку, втрата самоідентичності об'єкта тощо.

Щодо АСУ ОКІ, то найбільш актуальними загрозами при цьому є (табл.1.4):

Таблиця 1.4

Найбільш актуальні загрози АСУ ОКІ

Актуальні загрози	Обґрунтування актуальності	Заходи з усунення
Загрози фізичного доступу до АСУ ОКІ	Розміщення обладнання у загальних приміщеннях, куди мають доступ працівники підрядної організації (потенційні порушники відповідно до моделі порушника) Відсутність документованих процедур контролю доступу і супроводження обладнання, що може стати причиною збоїв та привести до помилок персоналу	СКУД Правила контролю доступу до АСУ ОКІ Правила контролю фізичної безпеки АСУ ОКІ Правила супроводження АСУ ОКІ
Загрози щодо НСД до АСУ ОКІ або розповсюдження злоякісних програм за рахунок підключення несанкціонованих пристроїв до мережі	Передбачуваний порушник, який може підключити власний мережевий пристрій шляхом під'єднання до мережі В мережі відсутні механізми, які дозволяють фіксувати підключення несанкціонованих пристроїв Підключення несанкціонованих пристроїв до мережі не надасть порушнику значних переваг для проведення атак	802.1x Правила безпеки мережі АСУ ОКІ

Під вплив таких загроз останнім часом все частіше підпадають такі ОКІ країн світу, як (рис.1.9) [15 – 18]:

Рис.1.9. Приклади впливу загроз на ОКІ країн світу

Методи реалізації загроз щодо АСУ ОКІ подано у табл 1.5.

Таблиця 1.5

Методи реалізації загроз АСУ ОКІ

Рівень доступу до АСУ ОКІ	Основні методи реалізації загроз			
	Загроза розкриття параметрів системи	Загроза порушення конфіденційності	Загроза порушення цілісності	Загроза порушення доступності
Носії інформації	Визначення типу і параметрів носіїв інформації	Викладення (копіювання) інформації Перехоплення ПЕМВН	Знищення машинних носіїв інформації	Виведення з ладу машинних носіїв інформації
Засоби взаємодії з носіями	Одержання інформації про: - програмно-апаратні засоби; - функції, що виконуються; - систему захисту	НСД до ресурсів АСУ Здійснення користувачем несанкціонованих дій Несанкціоноване копіювання ПЗ Перехоплення інформації, що передається каналами зв'язку	Внесення користувачем несанкціонованих дій в програми і дані Встановлення і використання нештатного ПЗ Зараження програмними вірусами	Прояв помилок проектування та розробки програмно-апаратних засобів АСУ ОКІ Обхід механізмів захисту АСУ
Подання інформації	Визначення способу подання інформації	Візуальне спостереження Розкриття подання інформації (дешифрування)	Внесення спотворень в подання інформації Знищення інформації	Спотворення відповідних синтаксичних і семантичних конструкцій мови
Зміст інформації	Визначення змісту інформації на якісному рівні	Розкриття змісту інформації	Упровадження дезінформації	Заборона використання інформації

Зважаючи на таке NIST США у 2014 році видав Рамковий документ щодо зміцнення кібербезпеки ОКІ [19], який включає в себе створення системи стандартів, інструкцій і практик для сприяння структурам приватного і державного сектора в управлінні ризиками в сфері захисту. Документ NIST позиціонується як модель, яка може сприяти «виробленню спільної мови міжнародного співробітництва в забезпеченні безпеки інформаційної критичної інфраструктури». Це, в свою чергу, вимагає [20 – 28]:

1) підвищення ступеня інтегрованості технологічних мереж;

2) активізації питань повязаних із забезпеченням їх безпеки;

3) врахування того, що засоби забезпечення безпеки традиційно відстають від можливостей зловмисників;

4) формування цифрових стратегій захисту ОКІ від антропогенно-техногенних загроз та природніх катаклізмів.

Це завдання може бути вирішеним за рахунок Інтеграції, наприклад, АСУ ОКІ в єдину корпоративну систему, переходу на використання стандартних протоколів на базі Ethernet на «низькому» рівні, передачі обслуговування на інсорс/аутсорс, в тому числі видалено через Internet та розвитку рольового рівня АСУ. Тобто, даючи об'єктивні передумови для підвищення ефективності життєдіяльності людства, розвиток ІКТ породжує цілий ряд складних і великомасштабних проблем. Одною з таких проблем є надійне забезпечення схоронності й встановленого статусу використання інформації, що циркулює й обробляється у комп'ютерних і телекомунікаційних системах, тобто її безпеки.

1.1.2 Уразливості програмно-апаратних засобів АСУ ОКІ та технології їх пошуку

Загрози, як можливі небезпечні прояви певної дії спрямованої проти об'єкта захисту, реалізуються через уразливості. Уразливість або слабкість (фактор) – будь-яка характеристика або властивість ОКІ, використання якої порушником може привести до порушення безпеки інформації на об'єкті інформаційної діяльності (ОІД) [29]. Уразливості, властиві ОКІ, невіддільні від них й обумовлюються недоліками процесу функціонування та властивостями архітектури ОКІ, протоколами обміну та інтерфейсами, програмним забезпеченням і апаратною платформою, умовами експлуатації та розташування ОКІ. Усунення або суттєве послаблення уразливостей впливає на можливість реалізації загроз безпеці АСУ ОКІ та інформації, яка в таких системах циркулює, накопичується і обробляється. Уразливості АСУ ОКІ можуть бути об'єктивними, суб'єктивними або випадковими. ***Об'єктивні*** уразливості залежать від особливостей побудови та технічних характеристик обладнання, що застосовується на об'єкті захисту. Повне усунення цих уразливостей неможливе, але вони можуть суттєво

послаблятися технічними та інженерно-технічними методами відбивання загроз безпеці інформації. ***Суб'єктивні*** уразливості залежать від дій співробітників і, в основному, вилучаються організаційними та програмно-апаратними методами. ***Випадкові*** уразливості залежать від особливостей середовища, яке оточує об'єкт захисту, та непередбачених обставин. Ці фактори, як правило, мало передбачувані і їх усунення можливе тільки при проведення комплексу організаційних та інженерно-технічних заходів із протидії загрозам безпеки.

За своєю суттю уразливості АСУ ОКІ можна розділити на чотири типи (табл.1.6):

Таблиця 1.6

Перелік уразливостей АСУ ОКІ

Уразливості зумовлені відсутністю передбачених моделлю управління керуючих документів	**Уразливості зумовлені відсутністю передбачених моделлю управління керуючих проектів**	**Уразливості зумовлені відсутністю передбачених моделлю управління технічних рішень**	**Уразливості пов'язані з конкретним ПЗ та/або пристроєм (у разі, якщо ПЗ власною розробкою організації)**
Відсутність політики парольного захисту	Відсутність моніторингу несправностей та помило, к системи	Відсутність технології захи сту конфіденційної інфор мації під час її передавання у формі приєднаних файлів	Наявність у користувачів прав привілейованого доступу до інформації
Відсутність процедури поводження з носіями інформації	Відсутність процедури періодичного перегляду існуючої системи класифікації інформації	Відсутність механізмів контролю дій системного адміністратора	Наявність у користувачів можливості відключення режиму безпеки (від імені адміністратора)
Відсутність процедури захисту мережі	Відсутність процедури доведення до відома працівникам, постачальникам і партнерам політики ІКБ	Відсутність механізмів щодо обмеження доступу персоналу до інформації	Наявність у користувачів можливості втручання у хід виконання певної операції на будь-якому етапі її виконання

уразливості зумовлені відсутністю передбачених моделлю управління керуючих документів;

уразливості зумовлені відсутністю передбачених моделлю управління керуючих процесів у випадку коли не виконуються передбачені моделлю управління керуючі дії;

уразливості зумовлені відсутністю передбачених моделлю керування технічних рішень (процедура повинна надавати можливість визначити задіяний у витоку інформації персонал та системи – відсутність засобів контролю витоку інформації);

уразливості пов'язані з конкретним ПЗ та/або пристроєм [2].

Найбільшу небезпеку становлять при цьому останні із наведених вище уразливостей, що пов'язані з конкретним ПЗ та/або пристроями. Так, наприклад, найбільшу загрозу при створенні АСУ ОКІ на етапах проектування, кодування і тестування становлять помилки ПЗ, що представлені в табл.1.7.

Таблиця 1.7

Помилки на етапах проектування і розробки ПЗ

Етап ЖЦ ПЗ	Помилки
Проектування	1) логічна непогодженість вимог;
	2) непогодженість протоколу взаємодії апаратури й програм;
	3) неточності алгоритмів;
	4) алгоритмічні закладки;
	5) впровадження неоптимальних інформаційних технологій;
	6) неточності в інтерфейсах між модулями
Кодування	1) нераціональна організація обчислювального процесу;
	2) створення програмної закладки, що може впливати на інші частини ПЗ
	3) синтаксичні помилки;
	4) логічні помилки.
Тестування	1) формування набору тестових даних, що не дозволяють виявити програмну закладку або помилки;
	2) відсутність тестів на випробування недокументованих можливостей програми;
	3)помилки в тестах

Тим не менш, не зважаючи на те, що наведені вище помилки є найбільш поширеними – їм приділяється найменша увага при оцінюванні безпеки АСУ ОКІ й, передусім, безпеки використовуваного програмного коду. При цьому, якщо на етапах проектування і тестування можливість уникнути багатьох помилок існує, то на етапі кодування це зробити набагато складніше бо саме через код програми зловмисник буде робити свої атаки використовуючи певні уразливості.

У цей час найпоширенішими видами уразливості в безпеці ПЗ є [30, 31]:

XSS (Cross-Site Scripting)– вид уразливості ПЗ (Web додатків), при якій на генерованій сервером сторінці, виконуються шкідливі скрипти, з метою атаки клієнта;

XSRF / CSRF (Request Forgery) – вид уразливості, що дозволяє використовувати недоліки HTTP протоколу. При цьому зловмисники працюють за такою схемою:

- посилання на шкідливий сайт встановлюється на сторінці, що користується довірою в користувача;

- при переході по шкідливому посиланню виконується скрипт, що зберігає особисті дані користувача (паролі, платіжні дані й т.д.), або відправляє спам повідомлення від імені користувача, або змінює доступ до облікового запису користувача, для одержання повного контролю над нею;

Code injections (SQL, PHP, ASP і т.д.) – вид уразливості, при якій стає можливо здійснити запуск коду, що виконується, з метою одержання доступу до системних ресурсів, НСД до даних або виведення системи з ладу;

Server-Side Includes (SSI) Injection – вид уразливості, що використовує вставку серверних команд в HTML коді або запуск їх прямо із сервера;

Authorization Bypass – вид уразливості, при якій можливо одержати НСД до облікового запису або документів іншого користувача, тощо.

Розподіл дефектів безпеки програмного забезпечення за типами подано на рис.1.10, а динаміку зростання їх кількості в останні роки – на рис.1.11.

Рис. 1.10. Розподіл дефектів безпеки ПЗ Рис. 1.11. Динаміка зростання кількості дефектів безпеки ПЗ

Найбільш важливими джерелами їх виникнення нині є сторонні додатки (80%), операційні системи (13%) та апаратні пристрої – 4%, а сферами впливу - державний сектор, кредитно-фінансові організації, транспорт та енергетика. Так, наприклад, як у програмному забезпеченні АСУ ОКІ, так і в їх серверних додатках домінують останнім часом уразливості на кшталт *відмови в обслуговуванні*, *компрометації системи* та *підвищення привілей*. Їх статистика в провідних компаніях світу за 2019 рік подана на рис.1.12 [32 – 34].

Згідно статистики найкращою серед відомих таксономій уразливостей програм з точки зору розробника є реєстр CWE, а з точки зору адміністратора – реєстр CVE [35]. За даними Інституту SANS, MITRE і багатьох провідних експертів по безпеці ПЗ США і Європи найбільш розповсюдженими і критичними CWE помилками (уразливостями), які можуть створити серйозні проблеми для безпеки ПЗ нині визнані: • небезпечна взаємодія між компонентами (6 помилок); • небезпечне керування ресурсами (8 помилок); • проникний захист (11 помилок).

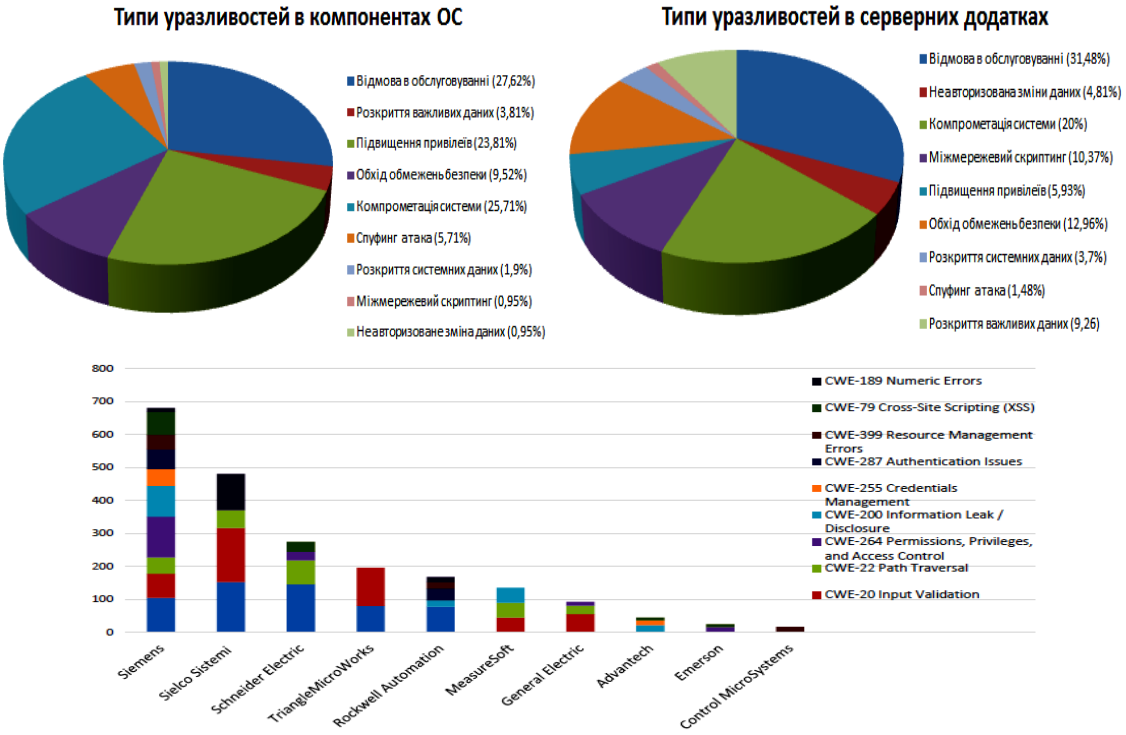


Рис.1.12. Типи та статистика уразливостей в ОС та серверних додатках АСУ

Перша категорія уразливостей (небезпечна взаємодія між компонентами) пов'язана з небезпечними шляхами між окремими компонентами, модулями, програмами, процесами, потоками або системами (табл. 1.8) по яких циркулює певна інформація.

Таблиця 1.8

CWE ID	Name
CWE-89	Некоректна нейтралізація спеціальних елементів, використовуваних у команді SQL («SQL-Ін'єкція»)
CWE-78	Некоректна нейтралізація спеціальних елементів, використовуваних у команді OS («Ін'єкція Команди OS»)
CWE-79	Некоректна нейтралізація вхідних даних при створенні веб-сторінки («міжсайтовий скриптинг»)
CWE-434	Необмежене закачування файлу небезпечного типу
CWE-352	Підробка запиту з перехресним посиланням («міжсайтовий скриптинг» - CSRF)
CWE-601	Перенапрямок з URL до недовіреного сайту («відкритий пере напрямок»)

Уразливості другої категорії (небезпечне керування ресурсами) пов'язані з некоректними способами керування ПЗ, що забезпечує створення, використання, передачу або видалення важливих системних ресурсів (табл. 1.9).

Таблиця 1.9

CWE ID	Name
CWE-120	Копіювання в буфер без перевірки розміру вхідних даних («Класичне переповнення буфера»)
CWE-22	Некоректне обмеження ім'я шляхи до каталогу обмеженого доступу («обхід каталогу»)
CWE-494	Завантаження коду без перевірки цілісності
CWE-829	Додавання функціональності з недовіреної сфери керування
CWE-676	Використання потенційно небезпечної функції
CWE-131	Неправильне обчислення розміру буфера
CWE-134	Неконтрольований рядок форматування
CWE-190	Цілочисельне переповнення або циклічне повернення

Уразливості на кшталт проникного захисту пов'язані із захисними методами, які часто неправильно використовуються або просто ігноруються (табл.1.10).

Таблиця 1.10

CWE ID	Name
CWE-306	Відсутність аутентифікації для критичної функції
CWE-862	Відсутність авторизації
CWE-798	Використання убудованих облікових даних
CWE-311	Відсутність шифрування критичних даних
CWE-807	Довіра ненадійним вхідним даним у прийнятті рішень по безпеці
CWE-250	Виконання з надмірними повноваженнями
CWE-863	Некоректна авторизація
CWE-732	Некоректне присвоєння дозволу на критичний ресурс
CWE-327	Використання зламаного або небезпечного алгоритму шифрування
CWE-307	Некоректне обмеження числа додаткових спроб аутентифікації
CWE-759	Використання однобічного хешування без використання випадкового числа (пароля)

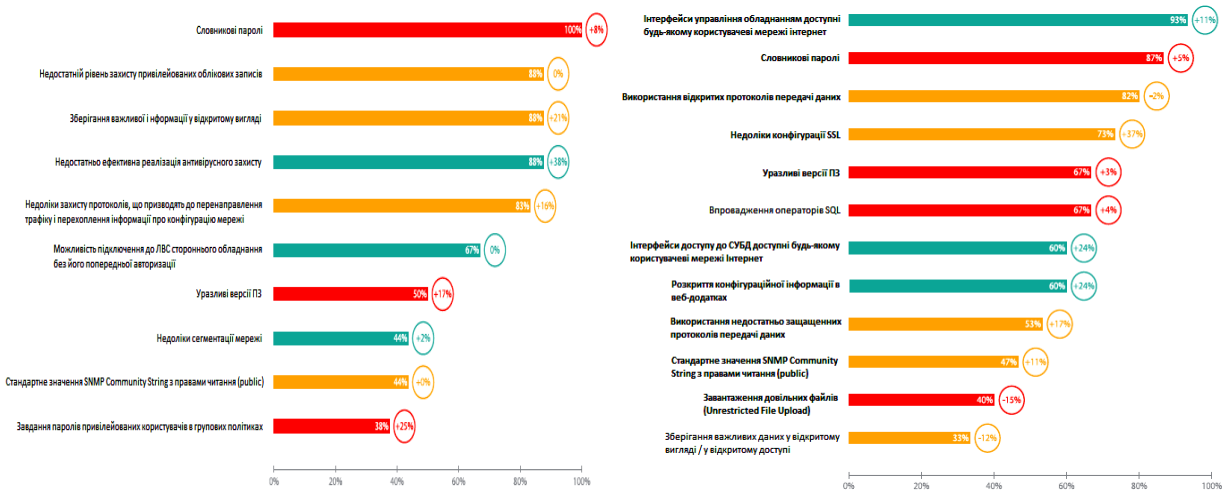
Відслідковуванням та накопиченням статистики уразливостей ПЗ займаються такі компанії, як NIST (National Institute of Standards and Technology, США), IBM,

Qualys, Cisco, WASC (Web Application Security Consortium), CERT (Computer Emergency Response Team) та багато інших. При цьому, наприклад, NIST підтримує актуальну базу даних уразливостей National Vulnerability Database (NVD), а також веде web-сайт бюлетеней уразливостей, що включає базову оцінку CVSS. Цю інформацію NIST надає на сайті: http://nvd.nist.gov/nvd.cfm. IBM Internet Security Systems (ISS) публікує бюлетені уразливостей, що включають базові та тимчасові оцінки CVSS на сайті: http://xforce.iss.net/xforce/alerts. Qualys публікує посилання на уразливості, які включають базові і тимчасові оцінки CVSS на сайті http://www.qualys.com/research/alerts/. Бюлетені уразливостей Cisco також включають базові і тимчасові оцінки CVSS, які публікуються компанією на сайті http://tools.cisco.com/MySDN/Intelligence/home.x. При цьому для доступу до інформації потрібен обліковий запис Cisco Connection Online. Tenable Network Security публікує плагіни для сканера безпеки Nessus. Вони включають базові оцінки CVSS, що публікуються на сайті http://www.nessus.org/plugins/.

Пошук уразливостей здійснюється, як правило, в ході тестування на проникнення шляхом дослідження внутрішнього і зовнішнього периметрів мережі, WEB-сайтів, баз даних, спеціалізованих додатків, безпроводових мереж тощо, а також проведення аналізу конфігурацій мережевих пристроїв, додатків і серверів на відповідність стандартам безпеки, тестування співробітників на стійкість до методів соціальної інженерії, моделювання фізичного проникнення до ОКІ, аналізу коду WEB-сайтів та додатків. При цьому перевіряється наявність і можливість використання вразливих місць, а саме:

- ✓ SQL Injection (використання операторів SQL);
- ✓ Source code injection (виконання довільного коду);
- ✓ OS Commanding (виконання команд ОС);
- ✓ Client-side Attacks (атак на клієнтів);
- ✓ Cross-Site Scripting, XSS (міжсайтового виконання сценаріїв);
- ✓ Content Spoofing (підміни вмісту);
- ✓ Buffer Overflow (переповнення буфера);
- ✓ механізмів авторизації та аутентифікації і інше.

Перевірка проводитися як вручну, так і з використанням різних сканерів від компаній MaxPatrol, Nessus, OpenVAC та інших. Програмні додатки цих компаній (сканер XSpider, систему моніторингу інформаційної безпеки Maxpatrol) активно використовує, наприклад, корпорація Positive Technologies (http://www.ptsecurity.ru/). Уразливості характерні для а) внутрішнього і б) зовнішнього pentest подано на рис.1.13 [36 – 40].



а) б)

Рис.1.13. Уразливості, характерні для а) внутрішнього і б) зовнішнього pentest

Приклад результату сканування наведено на рис.1.14.

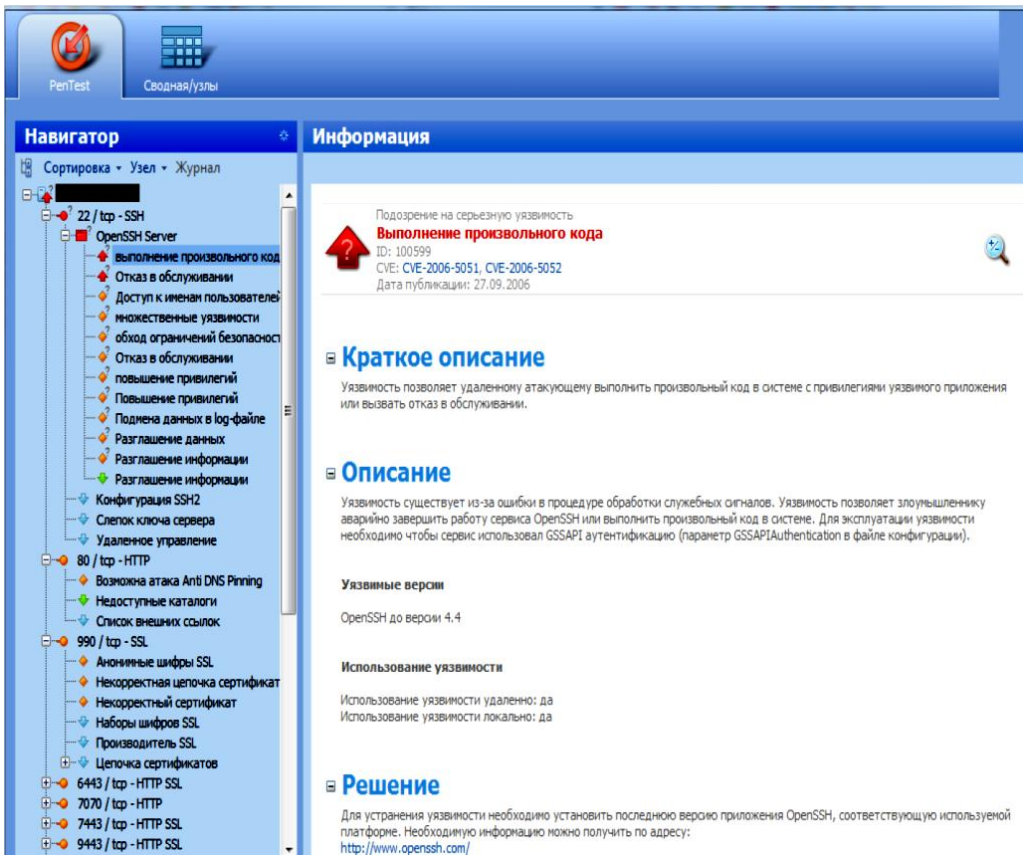


Рис.1.14. Приклад результату сканування уразливостей

1.1.3 Шляхи прогнозування відмов програмно-апаратних засобів АСУ ОКІ, оцінювання якості функціонування та наробітку на відмову таких систем

Прогнозувати кількість відмов програмно-апаратних засобів АСУ ОКІ, оцінювати та прогнозувати надійність таких систем при їх проектуванні і експлуатації, дозволяють математичні моделі. Зважаючи, що такі моделі мають зазвичай ймовірнісний характер, достовірність прогнозів залежить від точності початкових даних і глибини

прогнозування. Використання математичних моделей дозволяє ефективно проводити налаштування і випробування програмно-апаратних засобів, допомагає приймати раціональне рішення про час припинення налагоджувальних робіт.

На даний момент існує декілька таких моделей. Основними з них є:

- експоненціальна модель;
- модель розподілу Вейбулла;
- модель, що враховує дискретно понижувальну частоту появи помилок, тощо.

Експоненціальна модель застосовується за умови, якщо помилки ПАЗ розподіляються за законом Пуассона, проявляються у випадкові моменти часу та є незалежними. Час роботи між помилками визначається при цьому середнім часом виконання команди і середньою кількістю команд, що виконуються між помилками. Помилка, що є причиною спотворення результатів, за умови виявлення фіксується і виправляється після завершення тестування.

Якщо припустити, що на початку налаштування при $t = 0$ в ПАЗ містилося, наприклад, N_0 помилок, а після налаштування, яке тривало протягом певного часу t, в ПАЗ залишилося n_0 помилок, то кількість помилок, які було усунено дорівнюватиме $(n_0 + n = N_0)$. При цьому час t відповідає тривалості виконання налаштування ПАЗ, який для виявлення помилок не враховує простоїв, необхідних для аналізування результатів і проведення корегувань. Звідси інтенсивність виявлення помилок в ПАЗ dn/dt і абсолютна кількість усунених помилок пов'язані рівнянням:

$$\frac{dn}{dt} + bn = bN_0, \tag{1.1}$$

де b – коефіцієнт пропорційності.

Якщо припустити, що на початку налаштування при $t = 0$ помилки відсутні, то розв’язок рівняння (1.1) має вигляд:

$$n = N_0[1 - \exp(-bt)]. \tag{1..2}$$

При цьому кількість помилок ПАЗ, що залишилися $n_0 = N_0 - n = N_0 \exp(-bt)$, пропорційна інтенсивності виявлення dn/dt з точністю до коефіцієнта b.

Час безвідмовної роботи ПАЗ до відмови T або напрацювання на відмову, який розглядається як знайдене спотворення програмно-апаратних засобів, даних або обчислювального процесу, що порушують працездатність, дорівнює величині, зворотній інтенсивності виявлення відмов:

$$T = \frac{1}{dn/dt} = \frac{1}{bN_0} \exp(bt). \tag{1.3}$$

Якщо врахувати, що до початку тестування в ПАЗ містилося N_0 помилок і цьому відповідало напрацювання до відмови T_0, то функцію напрацювання до відмови від тривалості перевірок можна записати в такому вигляді: $T = T_0 \exp\left(\frac{t}{N_0 T_0}\right)$.

Якщо відомі моменти виявлення помилок t_1 і кожного разу в ці моменти виявляється та достовірно усувається одна помилка, то, використовуючи метод максимальної правдоподібності, можна отримати рівняння для визначення значення початкової кількості помилок N_0 $\sum_{i-1}^{n} \frac{n}{N_0-(i-1)} = \frac{n\sum_{i-1}^{n} t_i}{N_0 \sum_{i-1}^{n} - \sum_{i-1}^{n}(i-1)t_i}$, а також вираз для розрахунку коефіцієнта пропорційності: $b = \frac{n}{N_0 \sum_{i-1}^{n} t_i - \sum_{i-1}^{n}(i-1)t_i}$. В результаті можна розрахувати кількість помилок, що залишилися в ПАЗ, і середнє напрацювання до відмови $T_{\text{ср}} = 1/\lambda$, тобто отримати оцінку часу до виявлення наступної помилки.

В процесі налаштування і випробувань ПАЗ для підвищення напрацювання до відмови від T_1 до T_2 необхідно виявити і усунути Δn помилок.

Величина Δn визначається співвідношенням: $\Delta n = N_0 T_0 \left[\frac{1}{T_1} - \frac{1}{T_2}\right]$. (1.4)

Вираз для визначення затрат часу на проведення налаштування, що дозволяє усунути Δn помилок і відповідно підвищити напрацювання до відмови від значення T_1 до T_2 має вигляд: $\Delta t = \frac{N_0 T_0}{b} \ln (T_2/T_1)$.

<u>Друга модель</u> грунтується на процедурі врахування ступінчастого характеру зміни надійності при усуненні чергової помилки. Як головна розглядається функція розподілу часу напрацювання до відмови $P(t)$. Якщо помилки не усуваються, то інтенсивність відмов є постійною, що приводить до експоненціальної моделі розподілу [41]:

$$P(t) = \exp(-\lambda t). \quad (1.5)$$

Звідси щільність розподілу напрацювання до відмови T визначається за виразом:

$$f(t) = \lambda e^{-\lambda t}, \quad (1.6)$$

де $t > 0$, $\lambda > 0$ і $1/\lambda$ – середній час напрацювання до відмови, тобто $T_{\text{ср}} = 1/\lambda$.

Для апроксимації зміни інтенсивності від часу при виявленні і усуненні помилок використовується функція такого вигляду:

$$\lambda(t) = \lambda \beta t^{\beta-1}. \quad (1.7)$$

Якщо $0 < \beta < 1$, то інтенсивність відмов знижується при налагодженні або в процесі експлуатації. При такому вигляді функції $\lambda(t)$ щільність функції розподілу напрацювання до відмови описується двопараметричним розподілом Вейбулла:

$$f(t) = \lambda\beta t^{\beta-1}\exp(-\lambda t^{\beta}). \quad (1.8)$$

Розподіл Вейбулла досить добре відображає реальні залежності при розрахунку функції напрацювання до відмови.

Особливістю ***третьої моделі*** є застосування гіпотези про те, що інтенсивність відмов лінійно залежить від часу випробування t_i між моментами виявлення послідовних і-тої та (і - 1)-ї помилок:

$$\lambda(t_i) = \mathrm{b}[N_0 - (i-1)]t_i, \quad (1.9)$$

де N_0– початкова кількість помилок;

b – коефіцієнт пропорційності, що забезпечує рівність одиниці площі під кривою вірогідності виявлення помилок.

Для оцінки напрацювання до відмови застосовується вираз, який відповідає розподілу Релея:

$$P(t_i) = exp\left\{-b[N_0 - (i-1)]\frac{t_i^2}{2}\right\}, \text{ де } P(t_i) = P(T \geq t_i). \quad (1.10)$$

Щільність розподілу часу напрацювання до відмови з урахуванням рівняння (1.10) описується виразом:

$$f(t_i) = -P(t_i) = b[N_0 - (i-1)]t_1 exp\left\{-b[N_0 - (i-1)]\frac{t_i^2}{2}\right\}. \quad (1.11)$$

Використавши функцію максимальної правдоподібності, отримаємо оцінку для загальної кількості помилок N_0 і коефіцієнта b:

$$N_0 = \left[\frac{2n}{b} + \sum_{i-1}^{n}(i-1)t_i^2\right]\frac{1}{\sum_{i-1}^{n} t_i^2}; \quad (1.12)$$

$$b = \left[\sum_{i-1}^{n}\frac{2}{N_0-(i-1)}\right]\frac{1}{\sum_{i-1}^{n} t_i^2}. \quad (1.13)$$

Головними критеріями – мірою стратегії або інакше правилами згідно з якими формуються відповідні рішення та які дають можливість більш-менш об’єктивно оцінити якість функціонування АСУ ОКІ при цьому є критерії сумісності, розширюваності, масштабованості, продуктивності, відмовостійкості та ефективності. Вони передусім регламентують:

спроможність системи працювати якісно у реальному масштабі часу (**критерій *продуктивності***) з оцінюванням ступеню виконання поставленої перед нею мети (критерій *ефективності*);

здатність системи у заданих умовах функціонування з визначеними показниками якості виконувати покладені на неї функції при відмові її окремих елементів (**критерій *відмовостійкості***);

здатність системи включати в себе різноманітне програмне і апаратне забезпечення, а саме операційні системи, апаратні засоби і додатки від різних виробників (критерій *сумісності*);

спроможність щодо додавання до системи певних елементів – користувачів, комп'ютерів, додатків (критерій *розширюваності*), а також нарощування кількості її вузлів і довжини зв'язків (критерій *масштабованості*) тощо.

При цьому ***критерій продуктивності*** може характеризуватися, наприклад, показниками функціональної повноти, оперативності, пропускної здатності, рівня корисного використання ресурсів системи, а також затримки передачі інформації (інтервалом часу між моментом надходження пакета на вхід системи й моментом появи його на виході). Серед них показник функціональної повноти системи характеризує рівень автоматизації управлінських робіт:

$$K_f = \frac{П_a}{П_o}, \tag{1.14}$$

де $П_a$ – запити, отримувані автоматизовано; $П_o$ – загальна кількість запитів.

Показник оперативності ($T_i^{опер}$), або інакше часу реакції характеризує час, що витрачається на здійснення комплексу заходів від виникнення запиту користувача до мережевої служби системи до одержання ним відповіді. Оперативність залежить від завантаженості сегментів середовища передачі та активного мережевого встаткування (комутаторів, маршрутизаторів, серверів):

$$T_i^{опер} = T_i^{ген.зап.} + T_i^{очікув} + T_i^{обр.зап.} + T_i^{вид.відп.} + T_i^{корекц.}, \tag{1.15}$$

де $T_i^{ген.зап.}$ – час генерації запиту; $T_i^{очікув.}$ – час очікування; $T_i^{обр.зап.}$ – час обробки запиту; $T_i^{вид.відп.}$ – час видачі відповіді; $T_i^{корекц.}$ – час корекції на i-му етапі (кроці, циклі) звернення користувачів до мережевої служби; $i = \overline{1, K}$.

При цьому імовірність того, що тривалість сукупності вирішуваних АСУ ОКІ завдань не перевищить певного допустимого терміну $T^{доп.}$ визначається за формулою:

$$P\left(T^{опер.} \le T^{доп..}\right) = \Phi\left[\left(T^{доп.} - T^{опер.}\right) \Big/ \sqrt{\sum_{i=1}^{n} \sigma^2\left(T^{опер.}\right)}\right], \tag{1.16}$$

де $\Phi(x)$ – функція Лапласа, що задана в таблиці; $\sigma^2\left(T^{опер.}\right) = 0.4 \cdot \left(T_{\max}^{опер} - T_{\min}^{опер}\right)$.

Показник пропускної здатності системи характеризує обсяг максимально можливої кількості інформації, що може бути переданою по мережі за одиницю часу. Вона визначається самим повільним елементом системи яким, як правило, є маршрутизатор (наприклад: система працює швидко, без затримок, забезпечуючи за період (t) секунд (хвилин, годин) передачу (K) байт (Мб, Ггб, пакетів) інформації зі швидкість не менше, наприклад, (v) Мбіт/сек) тощо. У цей час широко використовується багатозначне визначення показника продуктивності процесора ЕОМ. Значення даного параметра вимірюється для різних класів завдань, обумовлених у цьому випадку процентним співвідношенням кількості різних арифметичних і логічних

операцій у розв'язуваних завданнях. Це надало користувачам можливість оптимального вибору обчислювальних систем для найбільш ефективного виконання розв'язуваних ними завдань. Точно так само багатозначне завдання й визначення відмовостійкості АСУ ОКІ дає можливість диференційовано підійти до проектування надійності її різних ділянок залежно від їхньої значимості й функцій.

Усі характеристики ***критерію відмовостійкості*** можна розділити на дві основні групи – характеристики достовірності ($Д$) та характеристики надійності ($Н$). Серед них характеристики достовірності визначають властивості АСУ ОКІ виконувати функції управління із заданою якістю в умовах впливу випадкових збоїв, а характеристики надійності – властивості системи при виникненні у ній відмов технічних засобів або при появі помилок у програмному та інформаційному забезпеченні, що приводять до переходу системи в стан повної або часткової непрацездатності. Головним серед характеристик достовірності є показник вірогідності передачі даних. Він визначає імовірність перекручування кожного переданого мережею біта інформації й, наприклад, для провідних ліній зв'язку становить 10^{-3}–10^{-4}, для кабельних – 10^{-5}–10^{-6}, для оптоволоконних ліній – 10^{-8}–10^{-9}.

1.2 Заходи захисту програмно-апаратних засобів АСУ ОКІ від несанкціонованої модифікації та незаконного використання

Відомо, що будь-яка інформація, яка є предметом власності, відповідно до вимог правових документів або вимог, встановлених власником інформації підлягає захисту. Захист при цьому являє собою як процес охорони, заощадження або порятунку від кого-небудь/чого-небудь неприємного, ворожого та небезпечного, так й передбачає сукупність методів, засобів і заходів, що застосовуються для недопущення або попередження таких дій.

Захист АСУ ОКІ озбивається на рішення двох основних груп задач. По-перше, заборона порушникам та/або іншим суб'єктам несанкціонованого доступу до засекреченої інформації у зловмисних цілях й, по-друге, своєчасне і повне задоволення інформаційних потреб, що виникають у процесі управлінської, інженерно-технічної, маркетингової та іншої діяльності, тобто забезпечення фахівців організацій (підприємств) секретної або конфіденційної інформацією. Вони реалізуються шляхом забезпечення технічного та/або криптографічного захисту інформації. Перший спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення втоку, знищення та блокування інформації, порушення цілісності та режиму доступу до неї, а другий – на приховування/відновлення змісту інформації, підтвердження її

справжності, цілісності, авторства тощо шляхом перетворення інформації з використанням спеціальних (ключових) даних [42, 43].

Питання технічного захисту розбиваються при цьому на такі класи завдань, як:

1) захист інформації від витоку технічними каналами (сукупності об'єктів розвідки, технічних засобів розвідки, за допомогою яких видобувається інформація та фізичного середовища, в якому поширюється інформаційний сигнал);

2) захист АС, зокрема АСУ ОКІ, і оброблюваної в них інформації від НСД. Під НСД в цьому сенсі розуміють доступ до інформації, що порушує правила розмежування доступу з використанням штатних програмно-апаратних засобів, що надаються АС (АСУ ОКІ). До головних способів НСД належать: безпосереднє звернення до об'єктів доступу; створення ПАЗ, що виконують звернення до об'єктів доступу в обхід засобів захисту; модифікація засобів захисту, що дає можливість здійснення НСД до ПАЗ; впровадження в ПАЗ АС (АСУ ОКІ) певних механізмів, що порушують структуру і функції цих систем й дозволяють здійснити певні несанкціоновані дії (табл.1.11).

Таблиця 1.11

Несанкціоновані дії щодо ПАЗ АСУ ОКІ

Звгрози	Несанкціоновані дії		
	Випадкові	Навмисні	
		Пасивні	Активні
Прямые	Невиявлені помилки програмного забезпечення КС; відмови і збої технічних засобів КС; помилки операторів; несправність засобів шифрування; стрибки електроживлення на технічних засобах; старіння носіїв інформації; руйнування інформації під впливом фізичних факторів (аварії і т.п.).	Маскування несанкціонованих запитів під запити ОС; обхід програм розмежування доступу; читання конфіденційних даних з джерел інформації; підключення до каналів зв'язку з метою отримання інформації («підслуховування» і / або «ретрансляція») при аналізі трафіку; використання терміналів і ЕОМ інших операторів; зважений виклик випадкових факторів (аварії і т.п.).	Включення в програми РПС, що виконують функції порушення цілісності та конфіденційності інформації та ПЗ; введення нових програм, що виконують функції порушення безпеки ПЗ; незаконне застосування ключів розмежування доступу; обхід програм розмежування доступу; виведення з ладу підсистеми реєстрації та обліку; знищення ключів шифрування і паролів; підключення до каналів зв'язку з метою модифікації, знищення, затримки і переупорядкування даних; виведення з ладу елементів фізичних засобів захисту інформації КС; зважений виклик випадкових факторів.
Опосередковані	Порушення пропускного режиму і режиму секретності; природні потенційні поля; перешкоди і т.п.	Перехоплення ЕМІ від технічних засобів; розкрадання виробничих відходів (роздруківок); візуальний канал; підслуховуючі пристрої; дистанційне фотографування і т.п.	Перешкоди; відключення електроживлення; зважений виклик випадкових факторів.

До найбільш критичних засобів, втручання до яких створює передумови для порушення структури і функцій АСУ ОКІ, як правило належать [44 – 47]:

блоки безперебійного живлення, які дозволяють працювати на ЕОМ деякий час після виключення електричного струму;

спеціальні регістри для зберігання реквізитів захисту: паролів, ідентифікаційних кодів, грифів або рівнів секретності;

пристрої для шифрування/розшифрування інформації (криптографічні методи);

спеціальні комп'ютери разом із специфічним програмним забезпеченням (брандмауери), які обмежують або фільтрують доступ до інформаційної системи із глобальних мереж;

пристрої вимірювання індивідуальних характеристик людини (голосу, відбитків) з метою його ідентифікації;

схеми переривання передачі інформації в лінії зв'язку з метою періодичної перевірки адреси видачі даних.

Для їх захисту від нелегального використання доцільно застосовувати як програмно-апаратні, так й програмні методи. Застосування програмно-апаратних методів грунтується на спеціально виготовлених CD, DVD и апаратних ключах, під'єднуваних через USB-порт та розповсюджуваних разом з программою інсталяції. Застосування програмних методів захисту інформації від несанкціонованої модифікації та незаконного використання передбачає їх прив'язування до ПЕОМ певної конфігурації (тобто до конфігурації обладнання на якому цю програму встановили) шляхом введення ліцензійного ключа або проходження процедури активації й грунтується на використанні як засобів захисту, що вбудовані в ОС та клієнтські додатки, так і окремих програмних модулів, оболонок, середовищ тощо (рис.1.15).

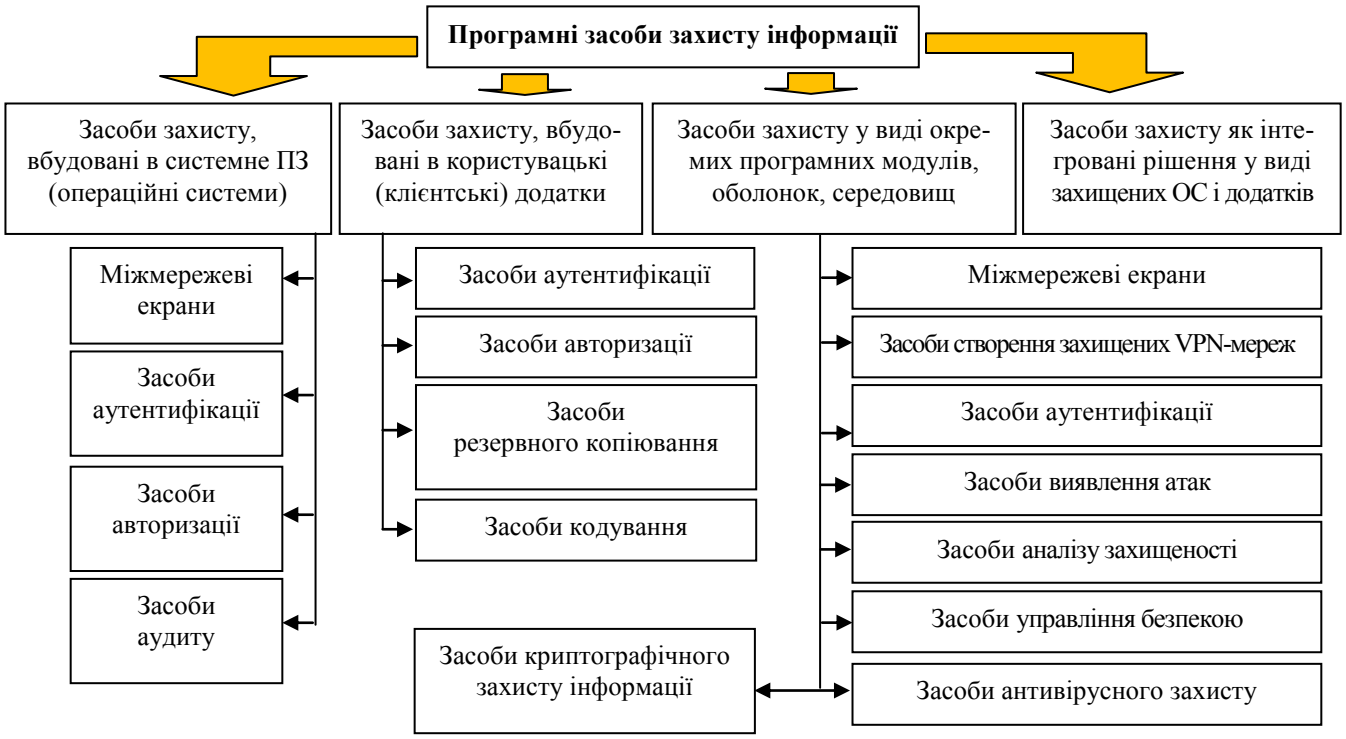


Рис.1.15. Програмні засоби захисту інформації в АСУ ОКІ

При цьому найчастіше для вирішення цих завдань застосовуються процедури упаковування та/або шифрування вихідного коду, обфускації вихідного коду, приховування викликів API-функцій та анти-відлагоджувальні методи (табл.1.12). Головним інструментом реалізації зазначених методів є так звані програми-протектори на кшталт VMProtect, Enigma Protector, Themida та Obsidium (табл.1.13).

Таблиця 1.12

Методи захисту ПАЗ АСУ ОКІ від несанкціонованої модифікації та незаконного використання

Упаковування та/або шифрування вихідного коду	**Обфускація вихідного коду**	**Приховування викликів API-функцій**	**Анти-відлагоджувальні методи**
Процедура захисту інформації полягає в тому, що файл в якому вона міститься повністю або частково упаковується та/або кодується. Розпаковування (розкодовування) та переавання управління на оригінальний код відбувається в памяті ПЕОМ.	Процедура заплутування вихідного коду реалізується шляхом вставки сміттєвого коду, змінення потоку виконання вихідного коду та його багатократних мутацій, або ж перетворення вихідного коду в код абстрактної віртуальної машини	Процедура дозволяє шляхом приховування функцій, адреси яких не потрапляють до таблицьакпкдавання та/або спрямування прямого виклику API-функції на виклик внутрішньої функції приховати від дослідника список API, який використовує програми\а, що підлягає захисту	Процедура дозволяє шляхом застосування API-функцій (IsDebugger Present, CheckRemote Debugger Present) або пошуку за іменем процесу, класу вікна або утворюваним об’єктам ядра знайти відлагоджувальник

Таблиця 1.13

Програми-протектори

	Формат файлів, що пітримується	ОС, що пітримуються	Процедури			
			упаковування та/або шифрування вихідного коду	обфускації вихідного коду	приховування викликів API-функцій	анти-відлагоджувальні
VMProtect	x86/x64 EXE, DLL	Усі 32/64-разрядні ОС Windows	-	+	+	+
Enigma Protector			-	+	+	+
Themida			+	+	+	+
Obsidium			-	+	+	+

Вони використовуються для:

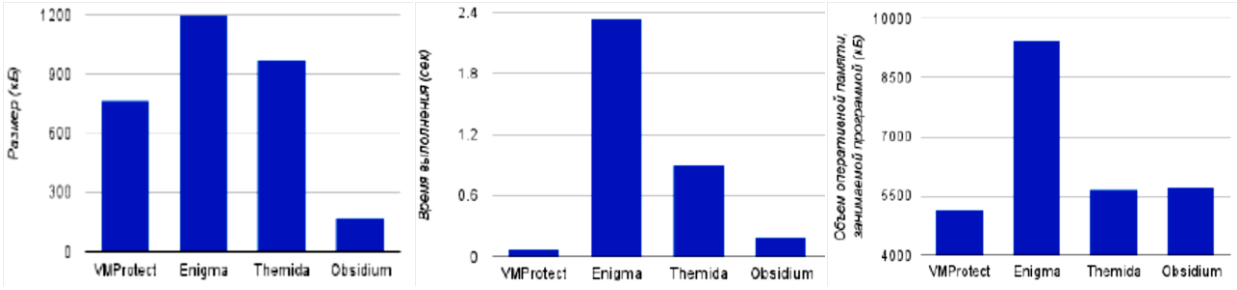
визначення та обмеження прав користувачів по доступу до системи;

шифрування та розшифрування інформації, що циркулює в системі;

фіксування дій користувачів щодо доступу до системи або інформації;

відновлення знищеної інформації на носіях, якщо знищення відбулося на логічному,а не на фізичному рівні, тощо.

Порівняльна характеристики зазначених програм-протекторів за параметрами а) «розмір файлу», б) «час виконання програми» та в) «обсяг оперативної пам’яті», отримані при захисті тестового додатку, наведено на рис. 1.16.



а) б) в)

Рис.1.16. Порівняльна характеристика програм-протекторів

Типовими утилітами, які застосовуються при цьому, наприклад, у програмі-протекторі Themida є:

CodeEncrypt (для шифрування/розшифрування вихідного коду);

SmartMetamorph та MutatorEngine (для мутації коду);

GarbageCode (для вставки мусорного коду);

VirtualMachine (для віртуалізація коду);

SecureAPIWrapper (для приховування таблиць імпорту);

MemoryGuard (для захисту пам'яті додатків від внесення змін в момент виконання);

DebuggerGuard (виявлення відлагоджувальників у системі),

AntiBreakpoints (для блокування точок зупинки при запуску додатку в середовищі відлагоджувальника);

AntiDumperPro (для блокування отримання «дампу» процесу захищеного додатку).

Враховуючи таке основні принципи захисту програмно-апаратних засобів АСУ ОКІ від несанкціонованої модифікації та незаконного використання може бути подано таким чином (табл. 1.14):

Таблиця 1.14

Принципи забезпечення технологічної безпеки ПАЗ АСУ ОКІ

Етапи життєвого циклу ПАЗ			
Проектування	Розробка	Випробування	Експлуатація
Комплексне забезпечення безпеки ПАЗ, що припускає розгляд проблеми безпеки інформаційно-обчис-лювальних процесів з урахуванням всіх структур АСУ, можливих каналів витоку інформації й НСД до неї, часу й умов їхнього виникнення, комплексного застосування організаційних і технічних заходів	*Регламентація технологічних етапів розробки ПАЗ*, що включає впорядковані фази проміжного контролю, специфікацію програмних модулів і стандартизацію функцій і формату подання даних	*Тестування ПАЗ* на основі розробки комплексів тестів, параметризуємих на конкретні класи програм з можливістю функ-ціонального й статистич-ного контролю в широ-кому діапазоні зміни вхідних і вихідних даних	*Збереження й обмеження доступу* до еталонів ПАЗ, недопущення внесення змін у них
Планове застосування засобів безпеки ПАЗ, що припускає перенос акценту на спільне системне проек-тування ПАЗ й засобів їх безпеки, планування їхнього використання в передбачуваних умовах експлуатації	*Автоматизація засобів кон-тролю керуючих і обчислю-вальних програм* на наявність дефектів, створення типової загальної інформаційної бази алго-ритмів, вихідних текстів і ПАЗ, що дозволяють ви-являти навмисні прог-рамно-апаратні дефекти	*Проведення натурних випробувань ПАЗ* при екстремальних навантаженнях з імітацією впливу активних дефектів	*Профілактично-вибіркове тестування й повне сканування* ПАЗ на наявність навмисних дефектів
Обґрунтованість забезпечення безпеки ПАЗ, що полягає в глибокому науково-обгрунтованому підході до прийняття проектних рішень по оцінці ступеня безпеки, прогнозуванню загроз безпеки, всебічній апріорній оцінці показників засобів захисту	*Послідовна багаторівнева фільтрація програмно-апаратних модулів* у процесі їхнього створення із застосуванням функ-ціонального дублювання розробок і поетапного контролю	*Здійснення "фільтрації"* ПАЗ з метою виявлення можливих навмисних дефектів певного приз-начення на базі створен-ня моделей загроз і від-повідних скануючих засобів	*Ідентифікація ПАЗ* на момент уведення його в експлуатацію відповідно до передбачуваних погроз безпеки ПАЗ і їх контроль
Достатність безпеки ПАЗ, що відбиває необхідність пошуку найбільш ефективних і надійних мір безпеки при одночасній мінімізації їхньої вартості	*Типізація алгоритмів*, програм і засобів ІБ, що забезпечує інформаційну, технологічну й програм-ну сумісність, на основі їх максимальної уніфікації по всіх компонентах і інтерфейсах	*Розробка й експериментальне відпрацьовування засобів верифікації* ПАЗ	*Забезпечення модифікації ПАЗ* під час їхньої експлуа-атації шляхом заміни окремих модулів без зміни загальної структури й зв'язків з іншими
Гнучкість керування захистом ПАЗ, що вимагає від системи контролю й керування забезпеченням ІБ ПАЗ оперативного й ефективного усунення загроз, які виникають в умовах різких змін обстановки інформаційної боротьби	*Централізоване керування БД проектів ПАЗ* й адміністрування технології їхньої розробки із твердим розмежуванням функцій, обмеженням доступу у відповідності із засобами діагностики, контролю й захисту	*Проведення стендових випробувань ПАЗ* для визначення ненавмисних помилок проектування й помилок розроблювача, що приводять до невиконання цільових функцій, а також виявлення потенційно "вузьких" місць у ПАЗ для руйнівного впливу	*Суворий облік й каталогізація* всіх супроводжуваних ПАЗ, а також збирання оброблюваної й збереженої інформації

Продовження табл.1.14

Принципи забезпечення технологічної безпеки ПЗ

Етапи життєвого циклу ПЗ			
Проектування	Розробка	Випробування	Експлуатація
Документованість технології створення ПАЗ, що припускає розробку пакета нормативно-технічних документів з контролю ПАЗ на наявність навмисних дефектів	*Використання тільки сертифікованих і обраних у якості єдиних інструмент-тальних засобів розробки ПАЗ* для нових технологій обробки інформації й перспективних архітектур обчислювальних систем	*Сертифікації ПАЗ АСУ по вимогах безпеки* з випуском сертифіката відповідності цього виробу вимогам технічного завдання	*Гнучке застосування додаткових засобів захисту ПАЗ* у випадку виявлення нових, непрогнозова-них загроз ІБ
Завчасність розробки засобів забезпечення безпеки й контролю виробництва ПАЗ, що полягає в попереджувальному характері мір забезпечення технологічної безпе-ки робіт в інтересах недопущення зниження ефективності системи безпеки процесу створення ПАЗ	*Блокування НСД* співвиконавців і абонентів державних мереж зв'язку, підключених до стендів для розробки ПАЗ	*Відпрацьовування засобів захисту від несанкціонованого впливу* порушників на ПАЗ	*Статистичний аналіз інформації* про всі процеси, робочі операції, відступах від режимів штатного функціонування ПАЗ
	Статистичний облік й ведення системних журналів про всі процеси розробки ПАЗ з метою контролю технологічної безпеки		

1.3 Формулювання і постановка наукової задачі дослідження

Виходячи з результатів проведеного аналізу можна стверджувати, що в Україні, як і в більшості країн світу нині:

відсутній єдиний підхід до дослідження основних понять інформаційної та кібербезпеки;

недостатньо розроблені такі початкові поняття, як «загроза» та «уразливість» об’єктів критичної інфраструктури;

відсутній нормативний документ, який би регламентував процес забезпечення безпеки на ОКІ та оцінки стану захищеності їх АСУ.

Такий стан справ не дозволяє повною мірою забезпечити відповідність необхідним організаційним, законодавчим, нормативним вимогам і міжнародним нормам, покращити ймовірність ідентифікації джерел загроз АСУ ОКІ та їх уразливостей, покращити результативність заходів, направлених на оцінку стану захищеності та на захист АСУ ОКІ**.** Тому, враховуючи вимоги викладені в «*Плані заходів щодо захисту державних інформаційних ресурсів»* від 5.11.2014 р., основною метою дисертаційної роботи є формування інтерактивної, інтегрованої та гнучкої інформаційної технології створення перспективних, багатофункціональних, надійних і захищених від стороннього кібернетичного впливу АСУ ОКІ, здатних за гнучкою схемою 24х7 безперебійно і гарантовано надавати необхідні послуги та виконувати потрібні функції в заданих режимах і умовах застосування.

Структурно-логічна схема проведення дослідження наведена на рис. 1.17.

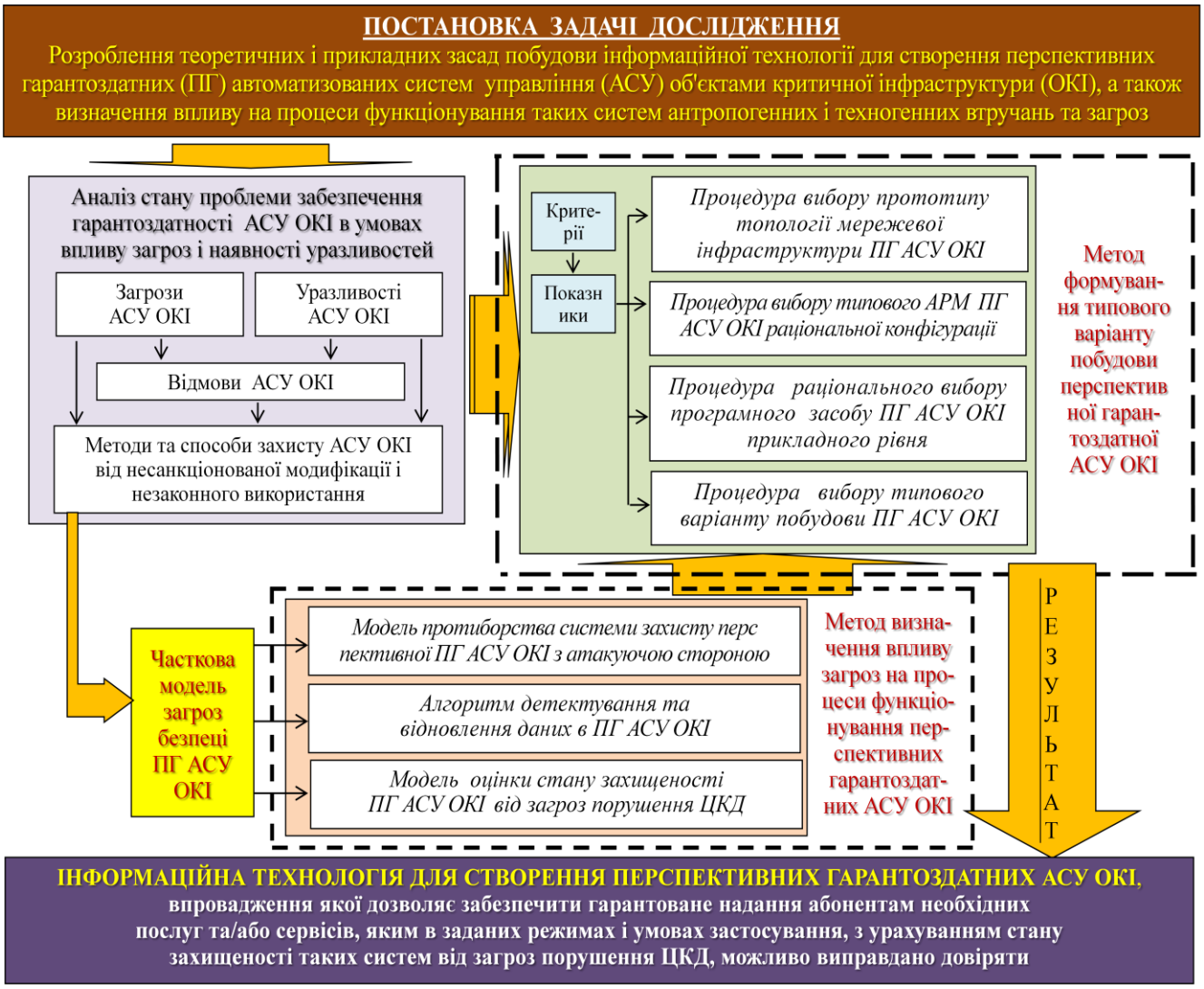


Рис. 1.17. Структурно-логічна схема проведення досліджень

Для досягнення мети, поставленої в роботі, необхідно:

1) розробити ***метод визначення впливу загроз на процеси функціонування перспективних гарантоздатних АСУ ОКІ***, впровадження якого шляхом реалізації *семантичної моделі протиборства системи захисту ПГ АСУ ОКІ з атакуючою стороною, процедури детектування та відновлення даних та моделі оцінки стану захищеності такої системи від загроз порушення ЦКД* **дозволяє**, на відміну від існуючих, **відслідкувати** вплив шкідливих програм, фальшивого ПЗ і злоякісних шифруючих кодів на ІТП в АСУ ОКІ, **відшукати** вразливості та/або істинні значення ключів, застосованих для шифрування даних в ПГ АСУ ОКІ, **оцінити** стан захищеності сформованого прототипу варіанту побудови ПГ АСУ ОКІ від впливу кібератак та **убезпечити** АСУ ОКІ від НСД до її ресурсів та інформації, що в ній циркулює;

2) удосконалити ***метод формування типового варіанту побудови перспективної гарантоздатної АСУ,*** впровадження якого *за рахунок розробки процедури вибору прототипу топології мережевої інфраструктури, процедури вибору*

типового АРМ раціональної конфігурації, процедури раціонального вибору ПЗ ПР та процедури вибору типового варіанту побудови ПГ АСУ ОКІ **дозволяє,** на відміну від існуючих, **організувати** доступ до мережі та надання обчислювальних ресурсів і послуг абонентам для спільного використання ними власних і зовнішніх ІР, **забезпечити** доступ користувачам до таких ІР, керування їх обміном, передачею та машинною переробкою, **автоматизувати** процеси пошуку і збору інформації у зовнішніх і внутрішніх джерелах, її реєстрації, трансформації та функціональної обробки, а також процеси захисту ІР в АСУ від кібернетичних загроз.

3) сформувати рекомендації щодо наукового та практичного використання результатів досліджень.

Висновки до першого розділу

Головну роль в процесах функціонування ОКІ країн світу та їх бізнес-структур останнім часом відіграє мережа Internet. Це веде до того, що ключові сегменти як ОКІ, так й бізнесу все частіше стають об'єктами деструктивних антропогенно-техногенних і природніх впливів, серед яких найбільшу шкоду за твердженням фахівців з міжнародної організації CERT надають (табл.1.15):

Таблиця 1.15

Перелік найбільш небезпечних загроз і уразливостей для ОКІ та бізнесу

Загрози			Уразливості	
Тип	Ймовірність шкоди (%)		Тип	Ймовірність шкоди (%)
Злоякісне ПЗ	68		Завантаження злоякісного ПЗ	54
Фішинг	54		Порушення внутрішньої безпеки співробітниками	47
APT- attack	43		Уразливості програмно-апаратного забезпечення	46
DoS/DDoS attack	38		Використання не штатних пристроїв та ПЗ	43
Brute force attack	35		Недостатня підготовка співробітників	39
Zero-day attack	35		Недостатній рівень підготовки фахівців з ІКБ	26

У 2013-2017 роках серед найбільш небезпечних загроз і уразливостей найактуальнішими для ОКІ та бізнесу були (рис.1.18) фішинг, шкідливі програми (віруси, сніфери, трояни), перевантаження та диверсії тощо, а серед уразливостей – необачність і необізнаність співробітників, застаріла система безпеки, НСД. Забезпечити стовідсотковий захист ОКІ та бізнесу за таких умов практично неможливо, але мінімізувати кількість уразливостей їх ПАЗ, зокрема АСУ від атак зловмисника – реально. Цьому сприяє наявність банку даних відмов і уразливостей, користування яким дозволяє класифікувати такі дефекти за певними ознаками. Огляд сучасних закордонних таксономій в галузі ІБ показав, що найбільш детально опрацьованою з

точки зору розробників є класифікація уразливостей за реєстром CWE, а з точки зору адміністратора – за реєстром CVE.

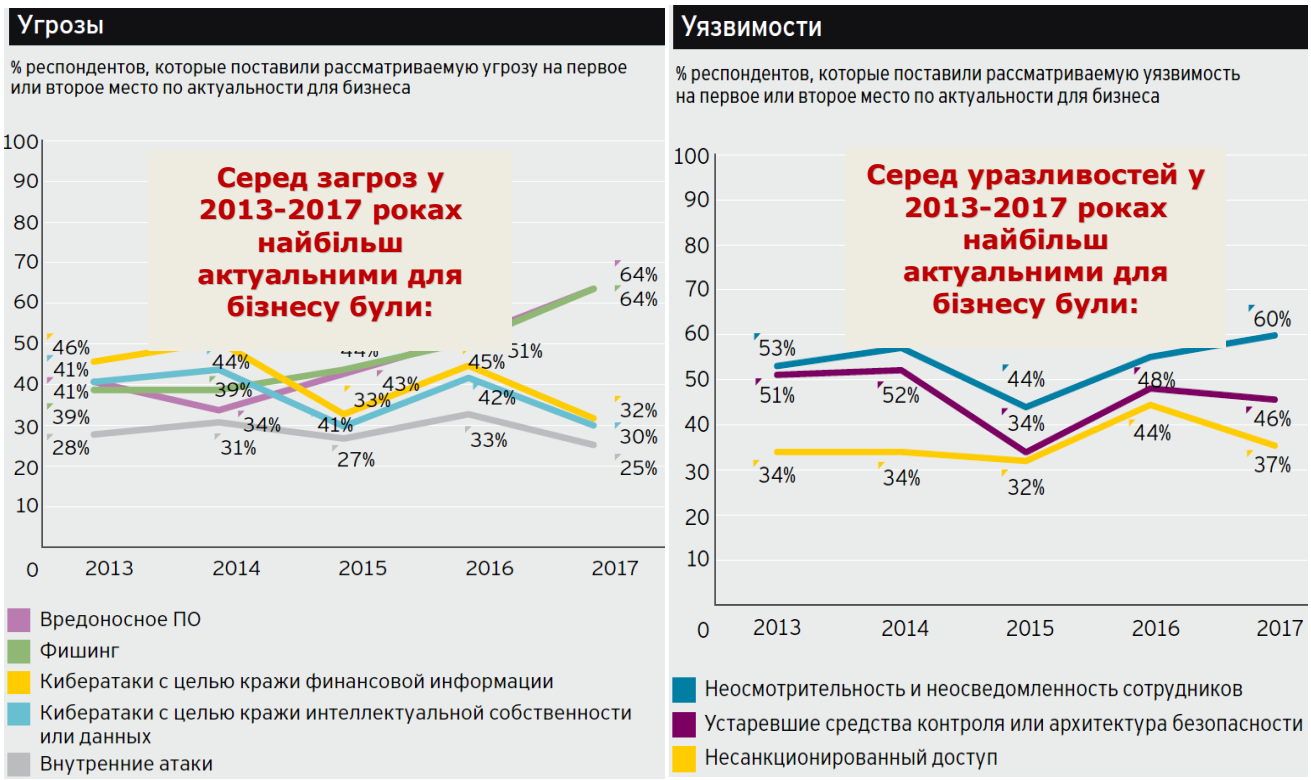


Рис.1.18. Актуальні загрози та уразливості АСУ ОКІ у 2013 – 2017 роках

Для захисту ПАЗ (АСУ) ОКІ та бізнесу від нелегального використання доцільно застосовувати як програмно-апаратні, так й програмні методи. Застосування програмно-апаратних методів грунтується на спеціально виготовлених CD, DVD и апаратних ключах, під'єднуваних через USB-порт та розповсюджуваних разом з программою інсталяції. Застосування програмних методів захисту інформації від несанкціонованої модифікації та незаконного використання передбачає їх прив'язування до ПЕОМ певної конфігурації (тобто до конфігурації обладнання на якому цю програму встановили) шляхом введення ліцензійного ключа або проходження процедури активації й грунтується на використанні як засобів захисту, що вбудовані в ОС та клієнтські додатки, так і окремих програмних модулів, оболонок, середовищ тощо. При цьому найчастіше для вирішення цих завдань застосовуються процедури упаковування, шифрування або оббфускації вихідного коду, приховування викликів API-функцій та анти-відлагоджувальні методи.

Список джерел, використаних у першому розділі

1. Бурячок В.Л. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства // Сучасна спеціальна техніка. – 2011. – № 3 (26). – С. 104–114.

2. Невойт Я. В. Метод оцінювання стану захищеності інформаційних ресурсів на основі дослідження джерел загроз інформаційній безпецs : автореф. дис. … канд. техн. наук : 21.05.01. Київ, 2016. 170 с.
3. Модель підготовки фахівців у сфері інформаційної та кібернетичної безпеки в закладах вищої освіти україни / V. L. Buriachok та ін. Information Technologies and Learning Tools. 2018. Т. 67, № 5. С. 277. URL: https://doi.org/10.33407/itlt.v67i5.2347 (дата звернення: 21.10.2020).
4. Даник Ю., Воробієнко П., Чернега В. Основи кібербезпеки та кібероборони. Одеса : ОНАЗ ім. О.С. Попова, 2019. 320 с.
5. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К.: НАУ, 2013. – 432 с.
6. Настанова національного космічного агентства України. Галузева система управління якістю. Гарантоздатність програмно-технічних комплексів критичного призначення. СОУ-Н НКАУ 0060:2010. – 60 с.
7. Харченко В. С. Гарантоздатність комп'ютерних систем: межа універсальності в контексті інформаційно-технічного стану // Радіоелектронні і комп'ютерні системи. – 2007. – № 8. – С. 8-16
8. А. Ю. Мартинов. Давоський економічний форум // Енциклопедія історії України : у 10 т. / редкол.: В. А. Смолій (голова) та ін. ; Інститут історії України НАН України. — К. : Наук. думка, 2004. — Т. 2 : Г — Д. — С. 280. — 518 с. : іл. — ISBN 966-00-0405-2.
9. В. В. Зимовець. Давоський міжнародний економічний форум // Всесвітній економічний форум // Енциклопедія сучасної України : у 30 т / ред. кол. І. М. Дзюба [та ін.] ; НАН України, НТШ, Координаційне бюро енциклопедії сучасної України НАН України. — К., 2003–2019. — ISBN 944-02-3354-X.
10. Бурячок В.Л., Гулак Г.М., Хорошко В.О. Завдання, форми та способи ведення воєн у кібернетичному просторі // Наука і оборона. – 2011. – № 3. – С. 35–42.
11. Медведовский И.Д. Атака через Internet. Содержание. [Електронний ресурс] / И.Д. Медведовский, П.В. Семьянов, В.В. Платонов. – Режим доступу: http://citforum.vision.am/internet/attack/toc.shtml.
12. Ільяшов О.А. До питання захисту інформаціно-телекомунікаційної сфери від стороннього кібернетичного впливу / О.А. Ільяшов, В.Л. Бурячок // Наука і оборона. – 2010. – № 4. – С. 35–40.

13. Пермяков О.Ю. Інформаційне протиборство: реалії і тенденції. / О.Ю. Пермяков, І.Є. Вернер // Арсенал XXI століття. – 2002. – №2. – С. 17 – 20.
14. A Solution-based Examination of Local, State, and National Government Groups Combating Terrorism and Cyberterrorism.By: Matusitz, Jonathan; Breen, Gerald-Mark. Journal of Human Behavior in the Social Environment, Feb2011, Vol. 21 Issue 2, p109-129, 21p. [Електронний ресурс]. – Режим доступу: http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN.
15. Руководство по кибербезопасности для развивающихся стран. [Електронний ресурс]. – Режим доступу: http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-r.pdf.
16. ITU's Global Cybersecurity Agenda: An International Framework for Cybersecurity. - Geneva : ITU, 2007. - 46 pp.. [Електронний ресурс]. – Режим доступу: http://www.itu.int/osg/csd/cybersecuritv/gca/index.html.
17. Про ратифікацію Конвенції про кіберзлочинність: за станом на 14.10.2010 р. / Закон, затверджений ВР України 07.09.2005, № 284-IV. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2824-15. Офіц. вид. – К.: Відомості Верховної Ради України від 10.02.2006.
18. Trend micro озвучила прогнозы по информационной безопасности на 2015 год. [Електронний ресурс]. – Режим доступу: http://www.infobezpeka.com/news/Trend-Micro-ozvuchila-prognozy-po-informacionnoy-bezopasnosti-na-2015-god/
19. National Institute of Standards and Technology. DRAFT NISTIR 8170 The Cybersecurity Framework.Implementation Guidance for Federal Agencies. Matt Barrett,Jeff Marron, Victoria Yan Pillitteri, Jon Boyens, Greg Witte, and Larry Feldman. [Online]. Available: http://csrc.nist.gov/publications/drafts/nistir-8170/nistir8170-draft.pdf. Accessed on: July 03, 2017.
20. В KASPERSKY LAB спрогнозировали действия киберпреступников на 2015 год. [Електронний ресурс]. – Режим доступу: http://www.infobezpeka.com/news/V-Kaspersky-Lab-sprognozirovali-deystviya-kiberprestupnikov-na-2015
21. MCAFEE LABS: в 2015 году предвидится активное использование эксплойтов и техник обхода. [Електронний ресурс]. – Режим доступу: http://www.antiviruspro.com/company/news/231/134617/

22. Аналитики GARTNER рассказали о том, что ждет мир через три-пять лет. [Електронний ресурс]. – Режим доступу: http://www.itsec.ru/newstext.php?news_id=106919
23. Отчет HP по информационной безопасности в 2013 году. [Електронний ресурс]. – Режим доступу: http://xakep.ru/2014/02/04/61990/
24. Рынок кибербезопасности вырастет до $170 млрд к 2020 году. http://digital.report/ryinok-kiberbezopasnosti-vyirastet-do-170-mlrd-k-2020-godu/
25. CyberEdge Group Отчет о противодействии киберугрозам за 2015 г. [Електронний ресурс]. – Режим доступу: https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/2015-cyberthreat-defense-report-executive-summary-ru.pdf.
26. ITU-T 2015. Security in Telecommunications and Information Technology. [Електронний ресурс]. – Режим доступу: http://www.itu.int/ITU-T/edh/files/security-manual.pdf
27. CERT-UA-Інформаційна-безпека. [Електронний ресурс]. – Режим доступу: http://cert.gov.ua/pdf/Брошура-CERT-UA-Інформаційна-безпека.pdf
28. В поисках асимметричных ответов: киберпространство в гибридной войне. [Електронний ресурс]. – Режим доступу: http://gazeta.zn.ua/internal/v-poiskah-asimmetrichnyh-otvetov-kiberprostranstvo-v-gibridnoy-voyne-_.html
29. Дмитрий Каталков. Уязвимости корпоративных информационных систем в 2015 году. [Електрон. ресурс]: – Режим доступа: https://www.ptsecurity.com/ru-ru/ics/Webinar_14042016.pdf
30. Киричок Р.В. Проблеми забезпечення контролю захищеності корпоративних мереж та шляхи їх вирішення / Складанний П.М., Бурячок В.Л., Гулак Г.М., Козачок В.А./ Науковий журнал «Наукові записки Українського науково-дослідного інституту зв'язку. – 2016. – №3(43). с. 48 – 61
31. Статистика уязвимостей web-приложений за 2016 год. [Електрон. ресурс]: – Режим доступа: https://www.ptsecurity.com/ru-ru/download/WASS-SS-2016-ru.pdf
33. Безопасность АСУ ТП в цифрах. [Електрон. ресурс]: – Режим доступа: https://www.ptsecurity.com/upload/ptru/analytics/ICS-Vulnerability-2016-rus.pdf
34. Контроль защищенности и соответствия стандартам Positive Technologies. [Електрон. ресурс]: – Режим доступа: ftp://ftp.software.ibm.com/software/security/products/qradar/ documents /iTeamaddendum/m_vuln_MaxPatrol.pdf

35. Борсуковський Ю.В. Базові напрямки забезпечення кібербезпеки державного та приватного секторів / Ю.В.Борсуковський, В.Л.Бурячок, В.Ю.Борсуковська / Науково-технічний журнал «Сучасний захист інформації» Державного університету телекомунікацій. № 2(30), 2017, с. 93 – 95
36. Бурячок В.Л., **Бурячок Л.В.** Поняття кібервійни та розвідки інформаційно-телекомунікаційних систем у контексті захисту держави від стороннього кібернетичного впливу. Вісник воєнної розвідки. – № 26. – 2012. – С. 45–52.
37. Бурячок В.Л., Невойт Я.В., **Бурячок Л.В.** Вплив загроз антропогенного і техногенного характеру на стан безпеки ІТ-систем та соціальних інститутів провідних країн світу і України. Сучасний захист інформації. – К.: ДУТ, 2015. – № 4. – С. 29–43.
38. Бурячок В.Л., **Бурячок Л.В.,** Гадицький М.Г. Цифрова стратегія безпеки критично важливих об’єктів державної інформаційно-комунікаційної інфраструктури. Матеріали Регіональної конференції МСЕ для країн СНД та Грузії «Перспективи надання послуг на основі мереж пост-NGN, 4G и 5G. Організаційні і технічні рішення щодо їх побудови та захисту», ДУТ, 7-9.06.2017. – К.: ДУТ, 2017. – С. 105–108 (електронний ресурс)
39. ISO/IEC 9126-1:2001 Software Engineering – Product Quality – Part 1: Quality model (Інжиніринг програмного забезпечення – Якість продукту – Частина 1: Модель якості)
40. IEC 61508-4:1998 Functional safety of electrical/electronic/programmable electronic safety related systems – Part 7: Definitions and abbreviations (Функціональна безпека електричних/ електронних/ програмованих електронних систем, важливих для безпеки – Частина 7: Визначення та скорочення)
41. Василевський О., Ігнатенко О. Нормування показників надійності технічних засобів. Вінниця : ВНТУ, 2013. – 161 с.
42. Д.М. Андрущенко, Г.Л. Козина. Метод защиты программного обеспечения от незаконного использования. // Системи обробки інформації, 2010, випуск 7 (88). – С. 77 – 81
43. К.Ю. Попырко, О.Г. Шевченко. Способы защиты программного обеспечения от несанкционированной модификации. // Информационные управляющие системы и компьютерный мониторинг, 2013. – С.61 - 67
44. О.В. Казарин. Безопасность программного обеспечения компьютерных систем. – Москва: МГУЛ, 2003. – 212 с.

45. А.Г. Додонов, Д.В. Флейтман. Корпоративные информационные системы: обеспечение живучести. // Математичні машини і системи, 2005, № 4. – С. 118 – 130
46. А.И. Аветисян, А.А. Белеванцев, И.И.Чукляев. Технологии статического и динамического анализа уязвимостей программного обеспечения. Вопросы кибербезопасности №3(4) – 2014. – С. 20 -28
47. Д.Ю. Гужва. Концептуальная модель воздействия нарушителя на инфотелекоммуникационную систему. Вестник ТОГУ, 2008, №4 (11). – С. 239 – 246
48. Закон України «Про основні засади забезпечення кібербезпеки України». https://zakon.rada.gov.ua/laws/show/2163-19#Text
49. Постанова Кабінету Міністрів України від 9 жовтня 2020 р. N 943 «Деякі питання об’єктів критичної інформаційної інфраструктури». https://zakon.rada.gov.ua/laws/show/943-2020-п#n13
50. Постанова Кабінету Міністрів України від 19 червня 2019 р. N 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури». https://zakon.rada.gov.ua/laws/show/518-2019-п#Text

Розділ 2
МЕТОД ФОРМУВАННЯ ТИПОВОГО ВАРІАНТУ ПОБУДОВИ ПЕРСПЕКТИВНОЇ ГАРАНТОЗДАТНОЇ АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ ОБ'ЄКТАМИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Розвиток автоматизованих систем йде останнім часом шляхом ускладнення як за рахунок збільшення кількості елементів, що входять у систему, так і їх взаємозв'язків між собою. Прикладом таких складних систем нині можуть слугувати АСУ ОКІ. Згідно [1] вони являють собою сукупність інформаційних (організаційно-технічних систем, що реалізують технології обробки інформації з використанням технічних і програмних засобів й забезпечують вироблення певних управлінських рішень) і телекомунікаційних (власне технічних та програмних засобів, призначених для забезпечення обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб) систем, які у визначених умовах протягом заданого проміжку часу діють як єдине ціле та орієнтовані на забезпечення реалізації певних завдань і функцій, а саме:

виявлення інформаційних потреб та добору джерел інформації;

проведення заходів з організації збору інформації, її введення та виведення;

опрацювання інформації, оцінювання її повноти і значущості;

подання інформації у зручному для користувачів вигляді та організації зворотного зв'язку з нею;

використання інформації для оцінювання тенденцій, розробки прогнозів, оцінювання альтернатив рішень і дій, вироблення стратегій тощо.

Виходячи з того, що метою створення будь-якої АСУ є розгортання у гранично короткі терміни системи обробки інформації, яка відповідає заданим споживчим властивостям – одною із найважливіших проблем останнім часом є забезпечення високої якості їх функціонування. Аналіз теорії та практики забезпечення і підтримування необхідного рівня якості при розробці, виробництві та експлуатації АСУ дозволив сформувати і узагальнити низку протиріч, існуючих у цій царині. Найбільш значущими серед них є протиріччя між [2, 3]:

відносно високим рівнем розвитку засобів автоматизації та низьким науково-методичним рівнем досліджень таких властивостей якості АСУ, як сумісність, розширюваність і масштабованість;

необхідним рівнем продуктивності та обмеженими можливостями промислової бази з виробництва якісної елементної бази і комплектуючих виробів АСУ;

закладеним у конструкцію АСУ рівнем відмовостійкості та її необхідним рівнем;

появою нових, більш ефективних АСУ й відставанням у створенні власних

подібних систем з необхідним рівнем ефективності;

зростанням витрат на розробку, виробництво та експлуатацію АСУ і реальними економічними можливостями замовника тощо.

Все це обумовлює потреби у створенні АСУ, які б стали, наприклад, невід'ємним сегментом індустріального Інтернету речей, а також в заданих режимах та умовах застосування гарантовано забезпечували здатність ОКІ виконувати потрібні функції.

Провідні галузеві підприємства України, як і об'єкти критичної інфраструктури нашої держави протягом усього часу свого існування перебувають у постійному процесі формування власної мережевої інфраструктури, що базується на широкому застосуванні технічних засобів (ЛОМ), економіко-математичних методів та сучасного мережевого ПЗ. Зважаючи на стрімке зростання обсягів інформації та враховуючи бурхливий розвиток ІТ це зумовлює необхідність провадження кардинальних змін засобів та способів обміну інформацією, а також формування принципово нових корпоративних телекомунікаційних мереж для створення єдиного інформаційного середовища.

2.1. Процедура вибору прототипу топології мережевої інфраструктури перспективної гарантоздатної АСУ ОКІ

Основу автоматизованих систем становлять комп'ютерні мережі (КМ). Вони є варіантом співпраці людей і комп'ютерів, що забезпечує прискорення доставки та розподілене опрацювання інформації різного функціонального призначення. Комп'ютерні мережі складаються, як правило, мінімум із двох комп'ютерів (ПЕОМ), що виконують достатньо широке коло функцій. Основними з них є:

по-перше, організація доступу до мережі;

по-друге, спільне використання IP загального користування;

по-третє, керування обміном, передачею, збереженням і поновленням інформації;

по-четверте, надання обчислювальних ресурсів і послуг абонентам мережі.

По числу підключених до мережі вузлів, а також їхньому географічному розташуванню КМ поділяються на локальні, регіональні та глобальні [4]. Локальні мережі (*LAN - Local Area Network*) – це сукупність декількох ПЕОМ, що мають загальне середовище передачі даних та фізично розташовані близько один до одного (в рамках окремої організації або корпорації). Локальні мережі підтримують передачу даних на надзвичайно високих швидкостях. Регіональні мережі (*MAN - Metropolitan Area Network*) – являють собою кілька сотень, тисяч або більше ПЕОМ, розташованих на відносно вилученій відстані один від одного (у межах одного міста або області), що мають при цьому загальне середовище передачі даних /5/. Регіональні мережі працюють на швидкостях від середніх до високих. Глобальні мережі (*WAN - Wide Area Network*) – це сукупність регіональних мереж, зв'язаних комунікаційними

каналами. Як комунікаційні канали найчастіше використаються телефонні лінії, а також більш дорогі варіанти: оптоволоконні кабелі, супутникові канали тощо. Глобальні мережі працюють на найнижчих швидкостях передачі даних. Прикладом глобальної мережі служить мережа Internet. Кожна з цих мереж характеризується власною архітектурою (табл. 2.1), а саме: топологією мережі, забезпечуючим інтерфейсом, протоколами обміну інформацією, технічними та програмними засобами. Кожна із складових архітектури комп'ютерної мережі характеризує її окремі властивості і лише їх сукупність характеризує всю мережу загалом.

Таблиця 2.1

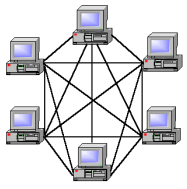
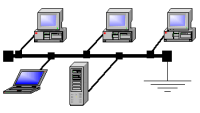
Архітекура комп'ютерної мережі та призначення її складових елементів

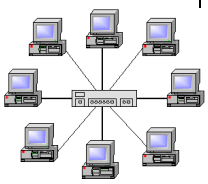
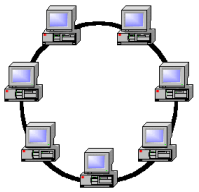
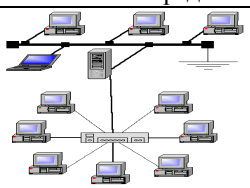
Архітектура комп'ютерної мережі та призначення її складових елементів	
Топологія	***Топологія мережі*** – це набір правил для фізичного з'єднання вузлів мережі й організації взаємодії мережних пристроїв. Топології мереж можна розділити на дві основні групи: повнозв'язні й неповнозв'язні. У мережі з повнозв'язною топологією кожний комп'ютер мережі прямо пов'язаний з кожним комп'ютером цієї мережі. Прикладом такої мережі є мережа стільникової топології. Більшість мережних топологій має неповнозв'язну структуру. До основних видів неповнозв'язних топологій можна віднести: шину, зірку, кільце й змішану топологію.
Інтерфейси	***Інтерфейс*** – це сукупність засобів сполучення функціональних елементів мережі. У ролі функціональних елементів можуть виступати як окремі пристрої, так і програмні модулі. Відповідно до цього існує апаратний та програмний різновиди інтерфейсів.
Протоколи	***Протокол*** – правило взаємодії функціональних елементів мережі.
Технічні засоби	***Мережеве технічне забезпечення*** – різноманітні пристрої (мережеві контролери, вузли комутації та ін.) з використанням яких виникає можливість об'єднання окремих ПЕОМ в єдину комп'ютерну мережу.
Програмні засоби	***Загальне*** (мережеві операційні системи тощо) та ***спеціальне*** (допоміжні або сервісні програми) ***програмне забезпечення –*** засоби, що керують роботою комп'ютерної мережі та забезпечують відповідний інтерфейс з користувачами.

Переваги та недоліки, що отримані на підставі аналізу топологій сучасних комп'ютерних мережних [1 – 7], приведено в табл. 2.2.

Таблиця 2.2

Переваги та недоліки класичних мережних топологій

Топології КМ		**Переваги**	**Недоліки**	**Графічне представлення**
Пов'я-зані	Стіль-никові	– висока надійність, обумовлена надмірністю фізичних зв'язків; – простота діагностики.	– потреба для кожного комп'ютера мережі великої кількості комунікаційних портів для з'єднання з усіма іншими ЕОМ; – необхідність виділення окремої електричної лінії зв'язку для кожної пари ЕОМ; – висока вартість стільникової мережі; – складність інсталяції й реконфігурації (додавання або видалення нових вузлів).	
Непов'язані	Шинні	– низька вартість; – простота розширення (простота підключення нових вузлів і об'єднання двох підмереж за допомогою повторювача); – відносно просте керування трафіком між підключеними пристроями; – достатня надійність (оскільки на функціонування справних вузлів не зможуть впливати несправні вузли або тракти, що поєднують їх із	– низька продуктивність; – низька надійність (часті дефекти кабелів і рознімань); – складність діагностики при розриві кабелю або відмові рознімання (любий дефект кабелю або рознімання приводить до непрацездатності всієї мережі. Для усунення такої ситуації необхідно зарезервувати канал або застосувати перемикачі для обходу вузлів, що відмовили); – важкість локалізації відмов із точністю	

		шиною).	до окремої компоненти, яку підключено до шини. Це зумовлюється відсутністю точок концентрації, через що проблема пошуку несправності стає важко розв'язуваною.	
	Зіркові	–легкість керування; –достатньо просте програмне забезпечення; –простий потік трафіка; –можливість швидкого пошуку несправностей; –відносну простоту та незначні витрати при потребі нарощування мережі (легкість створення підмереж шляхом придбання додаткового концентратора, приєднання до нього машин і з'єднання концентраторів між собою); –висока пропускна здатність порівняно із шинною топологією; –висока працездатність (вихід з ладу одного вузла або декількох вузлів не впливає на працездатність іншої мережі); –можливість використання замість хаба комутатора (для фільтрації трафіку, а також для моніторингу мережі); –можливість використання в одній мережі декількох типів кабелів.	– обмежена можливість збільшення числа вузлів мережі (обмежується кількістю портів концентратора); – залежність працездатності мережі від стану концентратора; – висока витрата кабелю (окремий кабель для підключення кожного комп'ютера); – висока вартість порівняно із шинною топологією (витрати на хаб і кабель); – виникнення "вузьких місць" у разі, коли трафіком керує пристрій, який розташований найвище; – мала надійність за відсутності технічного резервування; – часте виникнення конфліктних ситуацій, пов'язаних із втратою інформації в напрямі "згори - донизу" та "знизу - угору".	
	Кільцеві	– висока відмовостійкість (у технології FDDI); – відносна простота логічної організації; – нечасті перенавантаження, що притаманні ієрархічний або зіркоподібній топології. – при передачі даних (ретрансляції) не виникає втрати сигналу.	– низька надійність (відмова одного вузла може привести до непрацездатності всієї мережі, наприклад, у технології Token Ring); – додавання/видалення вузла змушує розривати мережу.	
	Змішані (наприклад, зірка-шина) та деревоподіб-ні.	Мережам змішаної топології притаманні певні переваги та недоліки, що характерні для їх складових. Серед відомих мереж змішаної топології більшу живучість мають деревоподібні топології. Відімкнення або вихід з ладу однієї з ліній або комутатора, як правило, не має значного впливу на працездатність частини локальної мережі, що залишилася. Однією з причин широкого використання мереж із деревоподібною топологією є також те, що ця структура найбільше відповідає структурі інформаційних потоків між абонентами мережі. Мережі з деревоподібною структурою застосовуються там, де неможливо безпосереднє застосування базових мережних структур у чистому вигляді.		
				

Рішення задачі щодо вибору прототипу топології мережевої інфраструктури гарантоздатної АСУ ОКІ може бути поділене на декілька доповнюючих один одного кроків, послідовність яких викладено нижче [4].

Крок 1. Структурування проблеми вибору прототипу топології МІ у вигляді ієрархії та виявлення найбільш важливих елементів, а саме (табл.2.3):

множини топологій, серед яких необхідно вибрати найкращу: Y_j, де $j=\overline{1,n}$. Для порівняння серед низки класичних мережних топологій (табл.2.2) оберемо чотири ($n=4$;),

а саме шинну (Y_1), кільцеву (Y_2),зіркову (Y_3) та стільникову (Y_4);

множини критеріїв, за якими має бути проведене порівняння $Y_j : K_t$, де $t = \overline{1,k}$, $k = 3$ (*в даному випадку критерій – це міра стратегії, або інакше правило згідно з якими формувались відповідні рішення*);

множини показників, що характеризуватимуть якість $Y_j : R_i$, де $i = \overline{1,m}$, $m = 10$ (*визначаються багатьма факторами та мають кількісний зміст. Вагові коефіцієнти даних показників змінюються в інтервалі від 1 до 10*). Для обчислювальних систем, які є ланкою контуру управління, в якості показників, як правило, розглядають: вартість, надійність, швидкодію, габарити, характеристики вхідних і вихідних сигналів тощо.

Таблиця 2.3

Критерії та показники оцінки сучасних мережних топологій

Критерії оцінки комп'ютерної мережі	**Показники**	**Позначення та формула розрахунку**		**Топологія**							
				Y_1		Y_2		Y_3		Y_4	
				R	b	R	b	R	b	R	b
Забезпечення дешевизни, K_1	Кабельна мережа	R_1	b_1	**10**	*9*	**7**	*6*	**6**	*5*	**1**	*0*
	Обладнання	R_2	b_2	**9**	*6*	**8**	*5*	**7**	*4*	**3**	*0*
	Монтаж	R_3	b_3	**10**	*8*	**8**	*6*	**5**	*3*	**2**	*0*
	Обслуговування	R_4	b_4	**1**	*0*	**2**	*1*	**10**	*9*	**5**	*4*
Забезпечення функціональності, K_2	Універсальність	R_5	b_5	**1**	*0*	**3**	*2*	**10**	*9*	**1**	*0*
	Діагностування	R_6	b_6	**1**	*0*	**2**	*1*	**10**	*9*	**10**	*9*
	Гнучкість	R_7	b_7	**1**	*0*	**2**	*1*	**7**	*6*	**1**	*0*
	Масштабованість	R_8	b_8	**8**	*7*	**3**	*2*	**10**	*9*	**1**	*0*
Забезпечення відповідності технічним вимогам, K_3	Швидкість роботи	R_9	b_9	**3**	*0*	**5**	*2*	**8**	*5*	**10**	*7*
	Захищеність від відмов	R_{10}	b_{10}	**3**	*0*	**3**	*0*	**7**	*4*	**10**	*7*

Коефіцієнт b_i, де $i = \overline{1,m}$, $m = 10$ (табл.2.3) має сенс і розраховується лише для критерію Севіджа для всіх Y_j за формулою: $b_{ij} = R_{ij} - \left(\min_i R_{ij} \right)$.

Крок 2. Вибір прототипу топології МІ ПГ АСУ ОКІ за класичними і похідними критеріями прийняття рішень в умовах невизначеності такими, як критерії Вальда, Севіджа та надзвичайного оптимізму (рис.2.1):

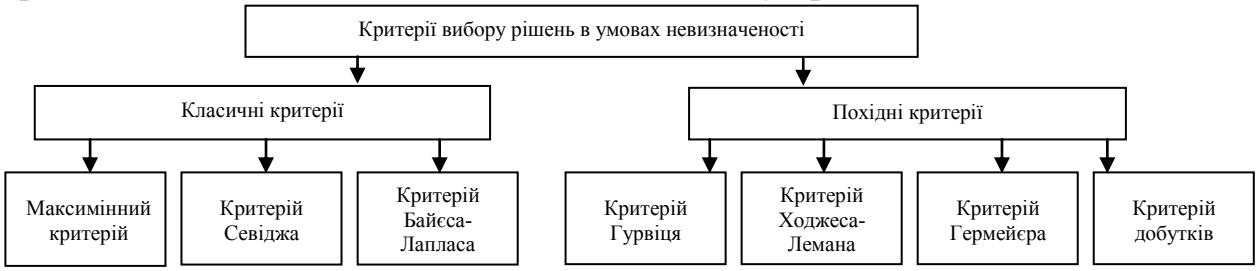


Рис. 2.1. Класифікація критеріїв вибору та прийняття рішень в умовах невизначеності.

Ієрархічна структура показників топологій сучасних КМ подана у табл.2.4.

Таблиця 2. 4

Ієрархічна структура показників топологій сучасних комп'ютерних мереж

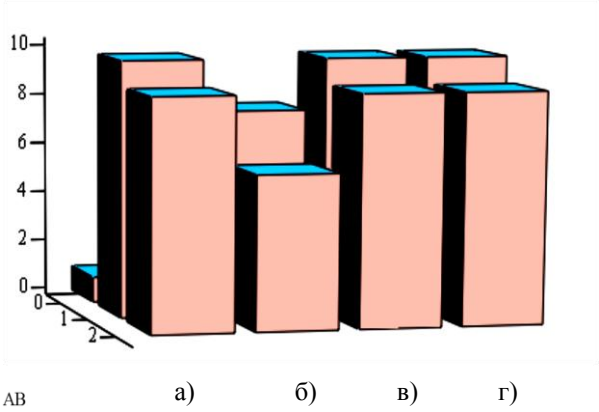
№ критерію на графіку MatchCad	Критерії порівняння існуючих альтернатив формування мережевої інфраструктури	Формула розрахунку	Топологія/позначення на графіку MatchCad							
			а)		б)		в)		г)	
			Y_1		Y_2		Y_3		Y_4	
			R	b	R	b	R	b	R	b
0	ВАЛЬДА (максимінний критерій)	$\min_j R_{ij}$	1		2		5		1	
		$\max_i\left(\min_j R_{ij}\right)$					5			
1	НАДЗВИЧАЙНОГО ОПТИМІЗМУ (максимаксний критерій)	$\max_j R_{ij}$	10		8		10		10	
		$\max_i\left(\max_j R_{ij}\right)$	10				10		10	
2	СЕВІДЖА (мінімаксний критерій)	$b_{ij} = R_{ij} - \left(\min_i R_{ij}\right)$	9		6		9		9	
		$\min_j\left(\max_i b_{ij}\right)$			6					

Зарезультатами обчислень (табл.2.4) отримаємо, що згідно критерію Вальда найбільш ефективним при створення перспективної АС може виявитися прототип Y_3, застосування чкого набагато спрощує процес проектування систем. За критерієм надзвичайного оптимізму такими можуть бути прототипи Y_1, Y_3 та Y_4. Критерій Севіджа пропонуватиме зосередити увагу дослідника, наприклад, на прототипі Y_2. Практичний же досвід створення КМ рекомендує зосередитись, як відомо, на прототипі Y_4. Це може пояснюватися, наприклад, тим, що:

по-перше, топологія Y_4 є перспективною але, водночас такою, що за сукупністю певних показників поступається топології Y_3;

по-друге, топології Y_1 та Y_2 на даний час взагалі є застарілими та малонадійними. Це пояснюється тим, що пошкодження кабелю на будь якому сегменті КМ створених за одним із цих підходів, призводить до зупинки всієї системи.

З отриманих результатів (табл.2.4) можна бачити, що використані критерії не дозволяють прийняти однозначне рішення щодо того яка з топологій, обраних для порівняння, буде найбільш раціональною при створенні ПГ АСУ ОКІ.



Крок 3. Щоб отримати відповідь напоставлене завдання та визначити місце кожного показника при виборі топології мережі під час створення перспективної АСУ проведемо додаткові розрахунки. Для цього може бути використано один із відомих методів прийняття рішень, таких, як:

математичне моделювання АСУ [8, 9]. Його перевага полягає в можливості проведення оцінювання статичних та динамічних характеристик таких систем. Обмеженість обумовлена тим, що ступінь достовірності моделей залежить від практичного та теоретичного досвіду їх розробників;

формування та дослідження узагальнених показників АСУ з використанням графоаналітичного методу, методу «прогресуючого еталону» тощо [10, 11]. Перевага цих методів полягає в можливості урахування великої кількості часткових показників єдиною числовою характеристикою – узагальненим показником, що дає можливість достатньо просто проводити порівняльне оцінювання таких систем. Обмеженість пов'язана з тим, що ці методи не враховують деякі економічні та виробничі фактори;

застосування «евристичних» (експертних) методів оцінювання, що базуються на використанні узагальненого людського досвіду - «колективної мудрості» [12 - 15].

При цьому саме методи експертних оцінок є визначальними при вирішенні складних завдань оцінювання та вибору будь-яких об’єктів, при аналізі та прогнозуванні ситуацій з великою кількістю значимих факторів. Їх застосовують, як правило за умови, що «… *вибір, обгрунтуванння та оцінювання результатів рішень не можуть бути виконані на основі точних розрахунків. Це забезпечує активну й цілеспрямовану участь фахівців на всіх етапах прийняття рішень, що уможливлює суттєве підвищення їхньої якості й ефективності*» [8]. Вони дають можливість більш глибоко вивчити явища, які слабко піддаються вивченню іншими методами, а також виявити найбільш важливе та істотне, не опускаючи тих деталей і взаємозв'язків, без яких не може бути побудована модель досліджуваної проблеми. Основними недоліками методів є суб'єктивізм думок експертів у відшукуваних оцінках та обмеженість їхніх суджень. Головна перевага зазначених методів, враховуючи незначні вимоги щодо наявності апріорної інформації про об'єкт дослідження, полягає у відносній простоті та зручності застосування для прогнозування практично будь-яких ситуацій.

Останнім часом найбільш поширеним серед відомих методів експертного оцінювання є метод аналізу ієрархій (МАІ) – систематична процедура для ієрархічного представлення елементів [16]. МАІ полягає в декомпозиції проблеми на більш прості складові та подальшій обробці послідовності суджень особи, що приймає рішення, по парних порівняннях (рис. 2.2). При цьому елементи задачі порівнюються попарно відносно їх впливу – «ваги», чи «інтенсивності», на загальну для них характеристику). В результаті може бути одержана відносна ступінь взаємодії елементів в ієрархії (у найбільш елементарному вигляді ієрархія будується з вершини (цілей), через проміжні рівні (критерії, від яких залежать наступні рівні) до самого низького рівня (який звичайно виявляється переліком альтернатив)). Отримані судження потім виражаються чисельно.

Рис. 2.2. Схема проведення досліджень з використанням методу аналізу ієрархій

Метод поєднує в собі процедури багатокритеріального опису проблеми, синтезу різних міркувань, отримання пріоритетності критеріїв та знаходження альтернативних рішень. Його основне застосування – підтримка прийняття рішень за допомогою ієрархічної композиції задачі та рейтингування альтернативних рішень.

Алгоритм реалізації методу з метою вибору серед сукупності альтернативних рішень прототипу топології формування мережевої інфраструктури ОКІ являє собою систематизовану послідовність кроків, що подані нижче [4].

Крок 3.1. Структурування проблеми вибору прототипу топології МІ за;

множиною топологій (R), серед яких необхідно вибрати найкращу,

множиною критеріїв та множиною показників, що характеризуватимуть якість обраних топологій.

Для вирішення цього завдання скористаємося результатами, отриманими на першому кроці даного дослідження. При цьому будемо враховувати той факт, що кількість порівнюваних альтернатив за MAI доцільно обмежувати 8 - 9 об'єктами, а можливості експерта з опрацювання інформації доволі обмежені. За гіпотезою Міллса експерт одночасно може враховувати не більш ніж 7±2 елементи. Тому для обраних топологій обмежимось, як визначено в табл.2.3, трьома критеріями оцінки та не більше ніж чотирма показниками для кожного з них:

Критерії	**Показники**	
Забезпечення дешевизни	Кабельна мережа	Монтажні роботи
	Обладнання	Обслуговування
Забезпечення функціональності	Універсальність	Гнучкість
	Діагностичність	Масштабованість
Забезпечення відповідності технічним вимогам	Швидкість роботи	Відмовостійкість

Крок 3.2. Виконаємо процедуру попарного порівняння як самих топологій, так і притаманних ним критеріїв і показників. Практика показує, що парні порівняння – найбільш зручна для експертів форма вираження своїх переваг. Можливі ускладнення, яких експерт зазнає при здійсненні парних порівнянь, зводяться до мінімуму, а надмірність інформації, що утримується в заповнених матрицях, дає можливість в процесі наступної обробки значно зменшити вплив помилок експертів при попарному зіставленні цінностей як окремих функцій і критеріїв, так і порівнюваних об'єктів загалом.

При здійсненні парних порівнянь критеріїв і показників, що характеризують альтернативні топології МІ та власне й самих топологій за кожним критерієм окремо передбачається, що вони можуть бути задані як якісно, так і кількісно. Експерт, користуючись спеціальною вербально-числовою шкалою (табл.2.5) та формулою (2.1) заповнює матриці парних порівнянь

$$A_l = \begin{Vmatrix} a_{11}^{(l)}, a_{12}^{(l)}, \cdots, a_{1j}^{(l)} \\ a_{21}^{(l)}, a_{22}^{(l)}, \cdots, a_{2j}^{(l)} \\ \cdots\cdots\cdots \\ a_{i1}^{(l)}, a_{i2}^{(l)}, \cdots, a_{mm}^{(l)} \end{Vmatrix} \qquad (2.1)$$

де n - число експертів; m - кількість показників

$a_{jk}^{(l)}$, $j = \overline{1,m}$, $k = \overline{1,m}$ - результат порівняння l-м експертом j-го показника з k-м.

Таблиця 2.5

Оціночна шкала відносної важливості (ваг)

Інтенсивність відносної важливості a_{jk}	Визначення	Пояснення
1	Рівна важливість	Рівний внесок двох видів діяльності в обрану мету
3	Помірна перевага одного над іншим	Досвід і судження (експертний аналіз) дають легку перевагу одного виду діяльності над іншим
5	Істотна або велика перевага	Досвід і судження (експертний аналіз) дають велику перевагу одного виду діяльності над іншим
7	Значна перевага	Одному виду діяльності дається настільки велика перевага, що він стає практично значним
9	Дуже велика перевага	Очевидність переваги одного виду діяльності над іншим підтверджується найбільше
2, 4, 6, 8	Проміжні рішення між двома сусідніми судженнями	Застосовуються в компромісних випадках
Зворотні розміри цих чисел	Якщо при порівнянні одного виду діяльності з іншим отримано, наприклад, 3, то результат зворотного порівняння - 1/3.	

В результаті: отримаємо

1) матрицю парних порівнянь показників для оцінки топологій КМ;

2) матриці парних порівнянь розміром $x \times x$ власне самих топологій за кожним показником.

Крок 3.3. Визначимо власні значення кожної із сформованих матриць, їх максимальні значення та відповідні цим значенням власні вектори.

Сформуємо вектор власних значень матриць попарного порівняння показників R_i ($i=\overline{1,m}$, $m=10$) за кожним із критеріїв K_t ($t=\overline{1,k}$, $k=3$), тобто їх локальних пріоритетів та нормовану до одиниці матрицю AB_{ji}, сформовану з власних векторів матриць попарних порівнянь топологій МІ за кожним із показників. Сформуємо власний вектор локальних пріоритетів показників, що використовуються під час порівняння топологій МІ - XBB_i. При цьому має виконуватися умова про те, для кожної із сформованих матриць коефіцієнти їх відносної узгодженості мають знаходитися в межах 10 %. Це свідчитиме про те, що зазначені матриці сформовані правильно й можуть бути використані для подальших розрахунків.

Крок 3.4. Обчислимо глобальні пріоритети досліджуваних топологій МІ, що дозволять визначити місце кожної з них серед порівнюваних:

$$AB_j^{glpr} = \sum_{i=1}^{m} \left(AB_{ji} - XBB_i \right). \qquad (2.2)$$

Крок 3.5. За сукупністю показників AB_j^{glpr} та враховуючи їх важливість на очікуваний результат, серед можливих варіантів оберемо прототип топології МІ для створення перспективної гарантоздатної АСУ ОКІ. Для подальших досліджень, а саме з метою апробації методу формування типового варіанту побудови ПГ АСУ ОКІ вводимо позначення K_{MI}^{nad} та приймаємо, що $K_{MI}^{nad} = AB_{\max}^{glpr}$.

2.2 Процедура вибору типового АРМ раціональної конфігурації перспективної гарантоздатної АСУ ОКІ

Після обрання прототипу топології побудови мережевої інфраструктури наступним етапом створення перспективної гарантоздатної АСУ ОКІ має бути комплектування таких систем автоматизованими робочими місцями (АРМ) користувачів – керівників та виконавців (АРМ аналітика, АРМ забезпечення інформаційної безпеки, АРМ комплексу засобів криптографічного захисту мережі передачі даних, АРМ адміністраторів локальних обчислювальних мереж та баз даних тощо). Вони створюються на базі персональних комп'ютерів (ПК), типового або спеціалізованого периферійного обладнання, а також відповідного програмного забезпечення й надають, як відомо, можливість здійснювати:

накопичення, систематизацію і опрацювання особистої інформації;

спільну роботу над загальними документами в складі структурного підрозділу;

доступ до власних та зовнішніх інформаційних ресурсів;

передачу та отримання кореспонденції електронною поштою тощо.

Зважаючи на постійне зростання обсягів інформації, що останнім часом обробляється в АСУ ОКІ, а також значну вартість використовуваного в АСУ ОКІ сучасного високотехнологічного обладнання постає проблема щодо підвищення вимог до експлуатаційних та технічних характеристик таких АРМ. Нині ця проблема може бути розв’язана шляхом впровадження деякого уніфікованого у рамках однієї організації АРМ, що сприятиме забезпеченню сумісності апаратних і програмних платформ різних підрозділів, вирішенню ними певних завдань з інформаційного та інформаційно-аналітичного забезпечення керівництва, уникненню застосування необґрунтованих технологічних рішень, а також впровадженню в організації єдиної політики інформаційної та кібербезпеки [21].

За звичай, під АРМ розуміють [22] діалогові професійно-орієнтовані індивідуальні й групові (колективні) системи обробки інформації, що розташовуються безпосередньо на робочих місцях обслуговуючого персоналу і фахівців (користувачів АСУ ОКІ) та які призначені для автоматизації діяльності зазначених посадових осіб шляхом реалізації інформаційних технологій у процесах виконання ними встановлених функцій. В цьому випадку індивідуальні АРМ характерні здебільшого, як відомо, для обслуговуючого персоналу АСУ ОКІ та керівників різних рангів, а групові – для осіб, що готують інформацію для керівників різних рівнів і ланок управління. В них має бути забезпечена максимальна наближеність зазначених фахівців до машинних засобів обробки інформації та максимальна автоматизація рутинних процесів. Множина відомих нині АРМ, може бути класифікована при цьому за такими ознаками: функціональними (наукова діяльність, проектування, виробничо-технологічні процеси, організаційне керування); експлуатаційними (індивідуальний, груповий, мережний); кваліфікаційними (професійні, непрофесійні) тощо. Їх структура та принципи функціонування такі, як системність, гнучкість, стійкість, ефективність, ергономічність, максимальна орієнтація на кінцевого користувача, – вимагають розробки сукупності різних видів (компонент) забезпечення: технічного, математичного, програмного, інформаційного, лінгвістичного, організаційного та інших (рис. 2.3) [23 - 25]:

а) компонент технічного забезпечення: засоби підготовки, накопичення, передачі, захисту та кодування інформації; структурована кабельна система та канали зв’язку; периферійні пристрої; тощо;

б) компонент математичного забезпечення: спеціальне математичне забезпечення, що поєднує математичні методи, моделі (процедури) і алгоритми та загальне математичне забезпечення (ЗМЗ), встановлене на АРМ;

в) компонент програмного забезпечення:

загальне програмне забезпечення (ОС АРМ користувачів; СУБД (СУБЗ) для реалізації функції організації та ведення БД (БЗ), забезпечення доступу при функціонуванні компонент тощо; текстові процесори для забезпечення створення та редагування спеціальних документів, електронних таблиць; графічні редактори для підготовки ілюстративних документів (матеріалів), а також інші прикладні програмні засоби реалізації додаткових функцій, що будуть визначені при проектуванні ІАС; утиліти для обслуговування АРМ (архіватори, драйвери зовнішніх пристроїв тощо); засоби підтримки телекомунікації; програми, що реалізують математичні процедури та алгоритми);

Рис.2.3. Типова структура АРМ

спеціальне програмне забезпечення (програми, що дозволять вирішувати специфічні задачі управління, які не можуть бути вирішені програмами ЗПЗ) та програмна документація;

ж) компонент інформаційного забезпечення: інформація, що необхідна для функціонування АСУ ОКІ, її зміст, обсяг, точність та ступінь деталізації, джерела інформації та її користувачів, характер і зміст інформаційних потоків; процедури збору, отримання, зберігання, обробки та документування інформації; форми організації і надання інформації користувачам та форм її представлення - позамашинної і внутрішньомашинної. Внутрішньомашинна інформаційна база - єдине, централізоване сховище даних певної предметної області, яке містить інформацію, необхідну для розв'язування зазадалегідь визначеного комплексу задач і до яких матимуть доступ багато програм різного призначення. Позамашиннна інформаційна база - сукупність документів та повідомлень, призначених для обміну інформаціїю між виконавцем та системою. До неї відносяться вхідні та вихідні документи на паперових носіях, форми

екранів для введення інформації у внутрішньомашинну інформаційну базу;

з) компонент лінгвістичного забезпечення: методи та засоби обробки текстової інформації; термінологічні словники; правила формалізації даних (уніфікація вхідних форм, первинної і зведеної звітності; методичний апарат класифікації та кодування); класифікатори; засоби діалогової взаємодії посадових осіб із засобами автоматизації (опис переліку функцій посадових осіб при роботі з інформацією; опис інформації, що супроводжує дії посадових осіб; умови та обмеження виконання тих або інших функцій);

к) компонент організаційного забезпечення. Основним змістом організаційного забезпечення є питання, які конкретно визначають: загальний порядок розробки, формування і реалізації АСУ ОКІ, тобто організаційну систему її створення; діяльність учасників формування і реалізації АСУ; загальний порядок керівництва та координування формуванням АСУ ОКІ, тощо.

Саме наявність передусім програмно-апаратних видів забезпечення дозволить обрати певне уніфіковане АРМ, у якому **максимальне значення показника продуктивності** – $P_{prodykt}^{\max}$ буде більшим або дорівнюватиме гранично припустимому значенню даного показника - $P_{prodykt}^{dopyst}$ $\left(P_{prodykt}^{\max} \geq P_{prodykt}^{dopyst}\right)$, а **експлуатаційні витрати** ($C_{експл}$) та **витрати на капітальні вкладення** ($C_{вкл}^{капіт}$) **в уніфікований АРМ** будуть мінімальними. Послідовність формування раціональної конфігурації АРМ перспективної гарантоздатної АСУ ОКІ (рис.2.4) викладено нижче [26 - 29].

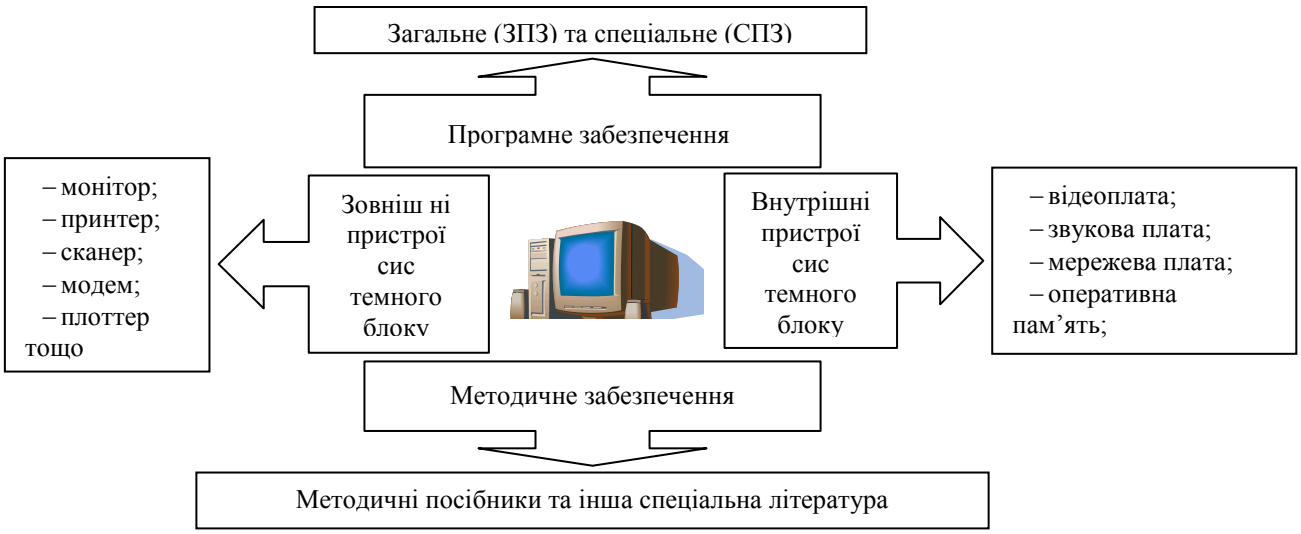


Рис. 2.4. Схема комплектації ПЕОМ для створення уніфікованого АРМ

Крок 1. Обираючи конфігурацію уніфікованого АРМ, призначеного для вирішення структурними підрозділами АСУ ОКІ завдань з інформаційного та інформаційно-аналітичного забезпечення керівництва, будемо вважати що, загальні витрати на створення такого АРМ ($C_{тех+прогр}^{АРМ}$) складаються з таких витрат:

$$C_{тех+прогр}^{АРМ} = \sum_{i=1}^{n} C_i^{TZ} + \sum_{j=1}^{m} C_i^{PZ}; \quad (2.3)$$

де C^{TZ} - вартість технічних засобів (ТЗ), наприклад, монітору, системного блоку, функціонального пристрою, тощо; C^{PZ} - вартість програмних засобів (ПЗ), наприклад, загального (ОС) та спеціального програмного забезпечення.

Крок 2. Визначення продуктивності кожної складової ТЗ і ПЗ, як лінійної функції від витрат, що необхідні для їх придбання:

$$P_i^{prodykt} = \mathrm{K}_i * C_i^{TZ},\ P_j^{prodykt} = \mathrm{K}_j * C_j^{PZ} \quad (2.4)$$

де K_i, K_j - нормуючі коефіцієнти, які фактично визначатимуть споживчу ефективність i-х технічних та j-х програмних засобів АРМ ($i = \overline{1,m}$, $j = \overline{1,n}$).

Крок 3. Формування матриці можливих конфігурацій для кожного i-го технічного та j-го програмного засобу АРМ ($i = \overline{1,m}$, $j = \overline{1,n}$). Побудуємо за даними матриць графіки залежності показників продуктивності від значень ціни та визначимо нормуючі коефіцієнти K_i (K_j), як котангенс кута нахилу апроксимуючої прямої до прямої показників продуктивності.

Крок 4. Формування цільової функції, яку необхідно мінімізувати

$$F\left(C_1^{TZ}, C_2^{TZ}, ..., C_m^{TZ}, C_1^{PZ}, C_2^{PZ}, ..., C_n^{PZ}\right) \xrightarrow[v]{} \min, \quad (2.5)$$

за обмежень:

$$P_{dop}^{prodykt} \le \mathrm{K}_i * C_i^{TZ} \le 100,\ P_{dop}^{prodykt} \le \mathrm{K}_j * C_j^{PZ} \le 100,\ C_i^{TZ} > 0,\ C_j^{PZ} > 0 \quad (2.6)$$

Вирази (2.5) та (2.6) відбивають класичне завдання лінійного програмування, де у якості вхідних даних мають бути задані значення обчислених на кроці №2 нормуючих коефіцієнтів для всіх складових уніфікованого АРМ та гранично припустиме значення показника їх продуктивності ($P_{dop}^{prodykt}$). Оптимальним рішенням задачі лінійного програмування називається рішення системи обмежень, що задовольняють умові за якої цільова функція приймає оптимальне (*max* або *min*) значення [29, 30]. Пошук оптимального рішення задачі лінійного програмування відбувається серед множини припустимих базисних рішень. Принципово це можна вирішити простим перебором, а саме:

знайти всі припустимі базисні рішення і для кожного з них обчислити значення цільової функції L;

вибрати припустиме базисне рішення, що відповідає мінімальному (максимальному) значенню лінійної функції L яке й буде оптимальним.

Перебір деякого скороченого набору базисних рішень доцільно здійснювати за рахунок: по-перше, упорядкованості перебору (за відомим базисним рішенням завжди можна знайти інше “більш краще” базисне рішення); по-друге, наявності ознаки, яка дає можливість констатувати, що дане базисне рішення є оптимальним без перегляду інших базисних рішень. Для цього доцільно скористатися можливостями універсальної системи математичних розрахунків «MATHCAD» (або ж табличного редактора *Microsoft Office Excel*, який забезпечує вирішення завдань лінійного програмування з багатьма змінними й обмеженнями). В результаті отримаємо значення припустимих витрат на закупівлю кожного з i-х технічних та j-х програмних засобів АРМ ($i=\overline{1,m}$, $j=\overline{1,n}$), добуток яких (2.3) становитиме частку від капітальних вкладень на впровадження АРМ:

$$C_{вкл}^{капіт} = C_{тех+прогр}^{АРМ} + C_{трансп} + C_{нал} + C_{пуск}, \qquad (2.7)$$

де $C_{трансп}$ - витрати на транспортування; $C_{нал}$ - витрати на налагодження; $C_{пуск}$ - витрати на запуск.

Крок 5. Оцінювання рівня окупності капітальних вкладень на впровадження АРМ раціональної конфігурації. Для цього скористаємось безрозмірним розрахунковим коефіцієнтом $K_P^{окупн}$, який являє собою відношення річної економії ($E_{рік}$) до витрат на впровадження АРМ ($C_{вкл}^{капіт}$) від початку й до кінця його життєвого циклу:

$$K_P^{окупн} = E_{рік} \Big/ C_{вкл}^{капіт}. \qquad (2.8)$$

де $E_{рік} = E_{оп} + E_{пр}$ - коефіцієнт річної економії від впровадження АРМ; (2.9)

$E_{оп}$ - коефіцієнт опосередкованої ефективності (характеризує якісні зміни, що можуть статися в результаті впровадження АРМ такі, наприклад, як: підвищення оперативності отримання інформації; скорочення термінів прийняття управлінських рішень тощо). Для його розрахунку застосовують, як правило, методи експертних оцінок;

$E_{пр}$ - коефіцієнт прямої ефективності. Може включати річний приріст прибутку, що викликаний, наприклад, зменшенням фонду заробітної плати його користувачів - керівників та виконавців: $E_{пр} = З_{безАРМ}^{фондЗП} - З_{зАРМ}^{фондЗП}$;

$З_{безАРМ}^{фондЗП}$ - річний фонд заробітної плати до впровадження АРМ;

$З_{зАРМ}^{фондЗП}$ - річний фонд заробітної плати після впровадження АРМ.

Для того щоб впровадження АРМ давало відчутні результати, значення показника $E_{рік}$ має бути значно більшим від нуля: $E_{рік} >> 0$ [23]. Це може бути досягнуто за умови, якщо: $\begin{cases} E_{оп} >> 0 & при \quad E_{пр} \geq 0 \\ E_{пр} >> 0 & при \quad E_{оп} \geq 0 \end{cases}$. (2.10)

При $E_{пр} \le 0$ обраний варіант впровадження АРМ вважається економічно недоцільним.

Крок 6. Порівняння чення $K_P^{окупн}$ з нормативним $K_{норм}^{окупн}$ [24, 25, 28]. Нормативний коефіцієнт економічної ефективності (окупності) капітальних витрат $K_{норм}^{окупн}$ встановлюється власником системи для кожного об'єкту, на якому буде впроваджуватися АРМ. Якщо $K_P^{окупн} \le K_{норм}^{окупн}$ та коефіцієнт річної економії від впровадження АРМ $E_{ефф}^{екон} \ge 0$, то конфігурація типового АРМ, обраного для комплектування перспективної гарантоздатної АСУ ОКІ є раціональною і не потребує уточнення. При цьому:

$$E_{ефф}^{екон} = E_{рік} - K_{норм}^{окупн} \cdot C_{заг} \qquad (2.11)$$

де $C_{заг} = C_{експл} + C_{вкл}^{капіт}$; (2.12)

$$C_{експл} = C_{осн}^{ЗП} + C_{доп}^{ЗП} + C_{СС} + C_{АО}^{тех+пр} + C_{рем} + C_{ел.ен.} + C_{матер}^{доп} + C_{АЗП}; \qquad (2.13)$$

$C_{осн}^{ЗП}$ – основна, а $C_{доп}^{ЗП}$ – додаткова заробітна плата працівників, зайнятих підготовкою й обробкою інформації, а також технічне обслуговування АРМ; $C_{СС}$ – відрахування органам державного соціального страхування; $C_{АО}^{тех+прогр}$ – амортизаційні відрахування від вартості технічних і програмних засобів; $C_{рем}$ – витрати на поточний ремонт АРМ; $C_{ел.ен.}$ – витрати на оплату споживаної електроенергії; $C_{матер}^{доп}$ – витрати на придбання допоміжних матеріалів, необхідних для експлуатації АРМ; $C_{АЗП}$ – амортизаційні відрахування із займаної площі.

Для подальших досліджень вводимо позначення та приймаємо, що $K_{АРМ}^{eff} = K_P^{окупн}$.

2.3 Процедура раціонального вибору програмних засобів прикладного рівня перспективної гарантоздатної АСУ ОКІ

Наступним етапом створення перспективної гарантоздатної АСУ ОКІ має бути проведення раціонального вибору програмних засобів (ПЗ) прикладного рівня (ПР) для комплектування системи. Це пояснюється тим, що для забезпечення якісного та ефективного функціонування робочих місць як керівників різних рівнів, так і користувачів у кожному АРМ мають бути інстальованими такі програмні засоби (ПЗ), які б задовольняли новим вимогам до інтерфейсу, підтримували меню, розвитий HELP, іконіку тощо. Це потребує від організацій різного напряму діяльності, зокрема об'єктів критичної інфраструктури, вирішення завдань щодо сертифікації та вибору серед існуючого розмаїття ПЗ такого, яке за параметрами і

функціями відповідало б потребам (вимогам) користувача (замовника) та відбивало б усі їх потреби, а також було спрямоване як на забезпечення роботи АСУ ОКІ, так й на розв'язання різнопланових завдань інформаційної діяльності.

В умовах сьогодення вирішення сформульованого вище завдання можливе лише за умови, якщо [29, 30]:

по-перше, встановлені повні, однозначні та верифіковані вимоги до ПЗ, що відбивають їх споживчі властивості;

по-друге, сформований план забезпечення якості ПЗ, включаючи методи та критерії контролю їх якості на всіх етапах розробки;

по-третє, визначені часові та інші ресурси для підготовки та проведення випробувань остаточної версії ПЗ та його компонентів.

Процедура вибору ПЗ ПР перспективної гарантоздатної АСУ ОКІ реалізується методами метод аналізу ієрархій (МАІ) та функціонально-вартісного аналізу (ФВА) й може бути поділена на декілька доповнюючих один одного етапів (рис.2.6), послідовність яких викладено нижче.

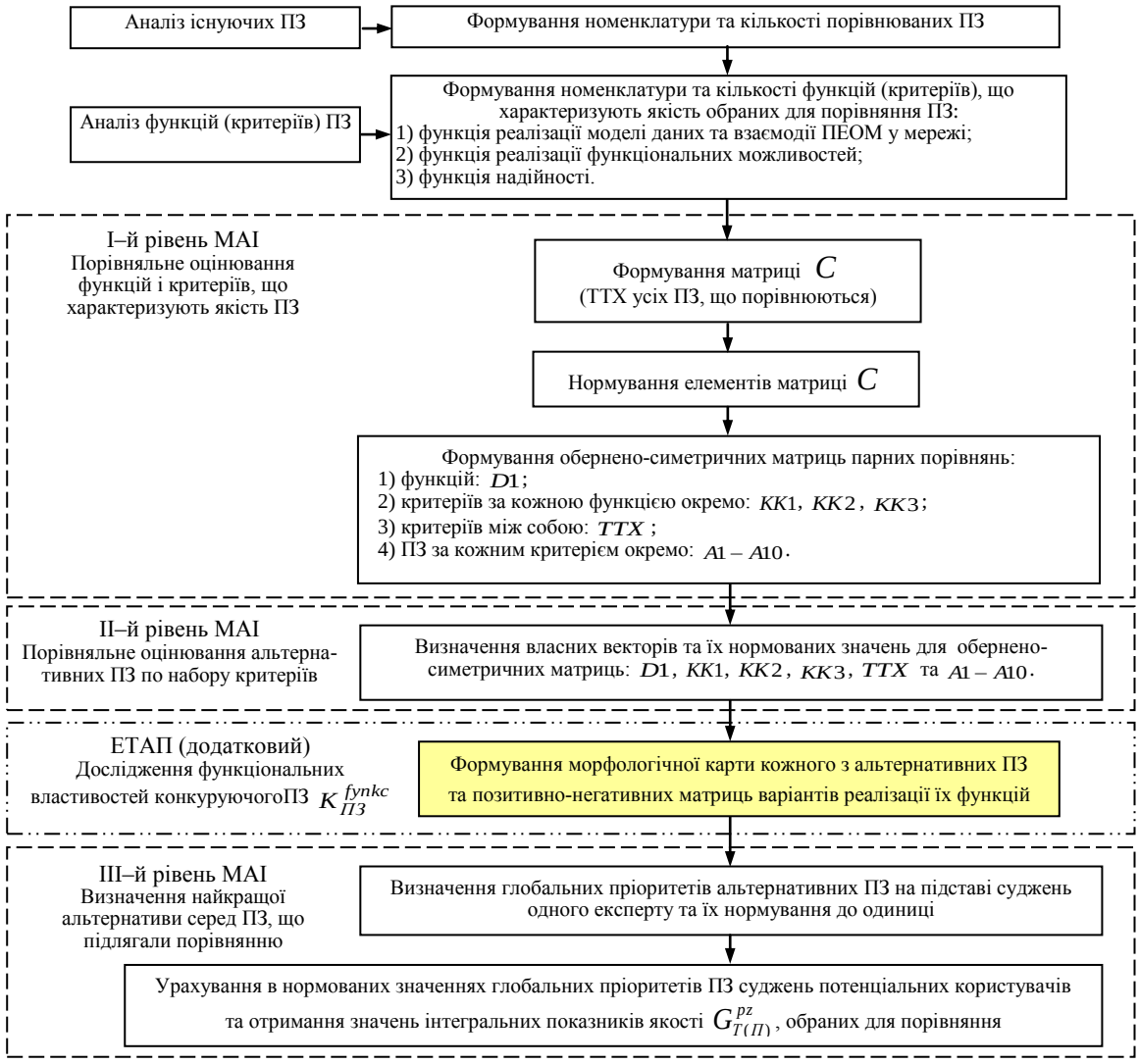


Рис. 2.6. Структурно-логічна схема методу порівняльного оцінювання ПЗ

Етап 1. Виходячи з викладеного визначимо вихідні дані, а саме:

множину альтернативних ПЗ (R), серед яких необхідно вибрати найкращу;

множину функцій (критеріїв), що характеризуватимуть якість обраних ПЗ.

Припустимо, що серед низки конкуруючих ПЗ однакового функціонального призначення нам необхідно обрати найбільш раціональний ПЗ, спрямований на розв'язання одного із завдань інформаційної діяльності. Зважаючи на те, що кількість порівнюваних альтернатив доцільно обмежувати 8 - 9 об’єктами, в якості досліджуваних оберемо: ПЗ 1 (R_1); ПЗ 2 (R_2); ПЗ 3(R_3). При цьому, враховуючи, що можливості експерта з опрацювання інформації, доволі обмежені й він не в змозі за гіпотезою Міллса одночасно враховувати більш ніж 7±2 елементи – для обраних R_1 - R_3 обмежимось, як і в попередньому випадку, 3 функціями ($N = 3$) та не більше ніж 5 критеріями для кожного з них, які певним чином характеризують властивості цих ПЗ, а також необхідні для комплексного оцінювання їх якості. При цьому під властивістю ПЗ, ієрархічне дерево яких наведено на рис. 2.7 [31, 36], слід розуміти його об’єктивну здатність, що може проявлятися при їх створенні, експлуатації й споживанні. Кількісна характеристика властивостей ПЗ виражається за допомогою відповідних факторів якості, які в загальному розумінні діляться на експлуатаційні, конструктивні та економічні.

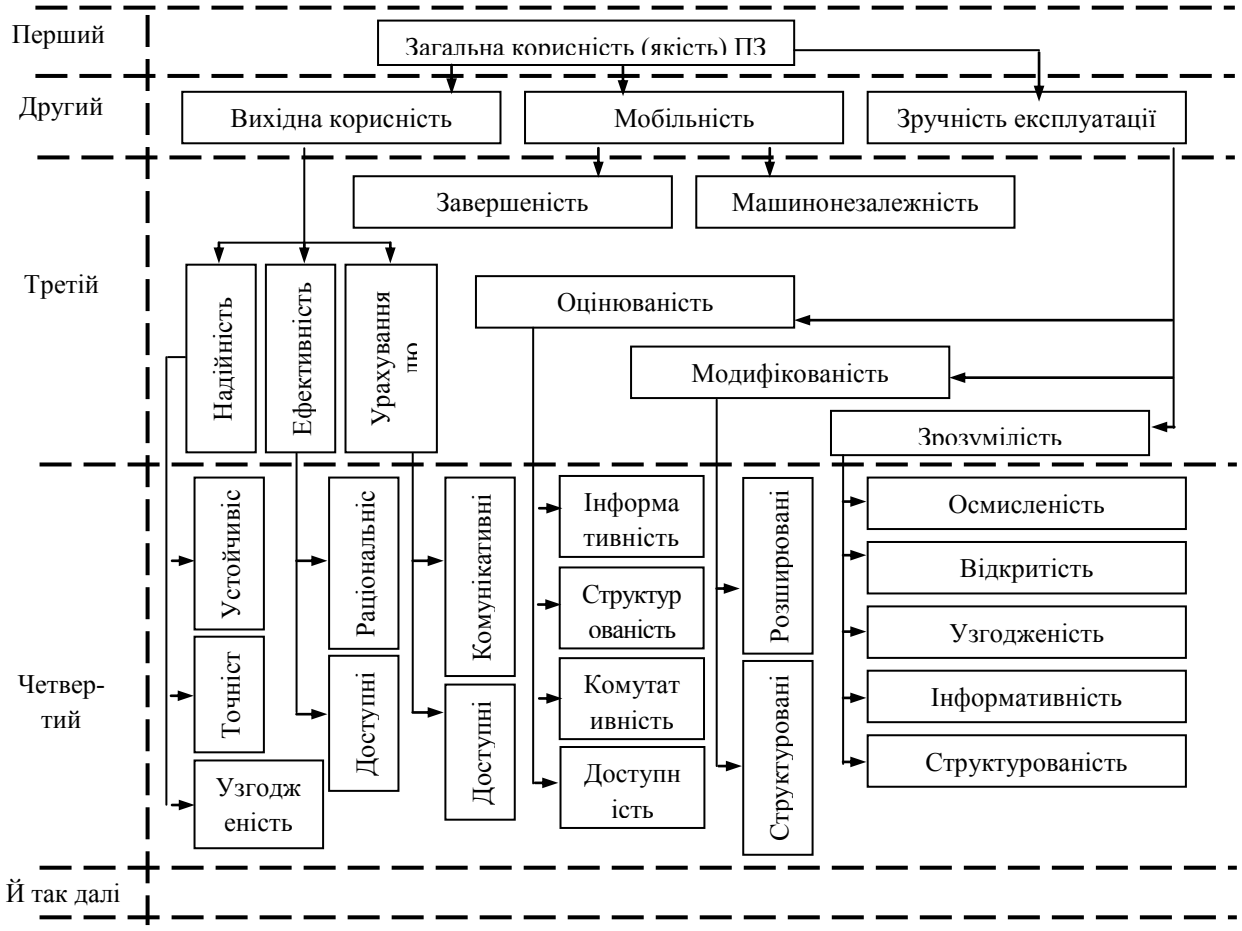


Рис. 2.7. Ієрархічне дерево властивостей програмного забезпечення

Група експлуатаційних факторів якості ПЗ включає *функціональність, надійність*, *зручність* (зрозумілість, ефективність освоєння, ергономічність), *ефективність* (раціональність за часом і по ресурсах), *супроводжуваність* (простота аналізу, змінюваність, стабільність, перевіряємість/тестованість, розширюваність), *мобільність* (адаптованість, гнучкість інсталяції, погодженість зі стандартами й правилами, замінюваність, переносимість), *практичність* (раціональна організація, продуманість, зрозумілість). Група конструктивних факторів якості ПЗ включає *складність* (структуру побудови ПЗ, взаємозв'язок її окремих частин), *модульність* (ступінь реалізації компонент ПЗ у вигляді модулів з певними обмеженнями й властивостями), *структурованість* (ступінь використання в програмі базових керуючих структур структурованого програмування), *тестованість* (ступінь пристосованості програми для організації перевірок правильності її роботи), *розмір* (використання ПЗ ресурсів оперативної й зовнішньої пам'яті ЕОМ), *точність* (розходження між дійсним та обчисленим значенням шуканої величини через погрішності методу, помилки чисельних методів рішення, помилки округлень та помилки, що обумовлені неточністю вихідних даних), *час реалізації на ЕОМ* (характеризує часовий інтервал між моментом надходження деякого набору вхідних дані програми й часом видачі відповідного результату) Група економічних факторів якості програм включає *вартість розробки* та *вартість експлуатації*.

Шкалу вимірів експлуатаційних субфакторів якості ПЗ, наведено в табл.2.7.

Таблиця 2.7

Шкала вимірів вибіркових експлуатаційних субфакторів якості ПЗ

Фактори та субфактори якості ПЗ	Міра	Шкала
Практичність		
Зрозумілість:		
- чіткість концепції ПЗ;	порядкова	Відм.; В
- демонстраційні можливості;	порядкова	гарна; Г
- наочність і повнота документації.	порядкова	задов.;З
Простота використання:		незад. Нз
- простота управління функціями;	порядкова	
- комфортність експлуатації;	порядкова	
- середній час уведення завдань;	секунди	1 - 1000.
- середній час відгуку на завдання.	секунди	1 - 1000.
Мобільність		
Адаптованість:		
- трудомісткість адаптації;	чол.\год.	1 - 100.
- тривалість адаптації.	години	1 - 100.
Простота установки:		
- трудомісткість інсталяції;	чол.\год.	1 - 100.
- тривалість інсталяції.	години	1 - 100.
Співіснування - відповідність:		
- стандартизація інтерфейсів з апаратним й операційним середовищем	порядкова	В/Г/З/Нз
Замінюваність:		
- трудомісткість заміни компонентів;	чол.\год.	1 - 100.
- тривалість заміни компонентів.	години	1 - 100.
Надійність		
Стійкість:		
- наробіток на відмову при наявності автоматичного рестарту;	години	10-1000.

Фактори та субфактори якості ПЗ	Міра	Шкала
- відносні ресурси на забезпечення надійності й рестарту.	%	10-90.
Відновлюваність:		
- тривалість відновлення.	хвилини	10-2 - 10.
Доступність-готовність:		
- відносний час працездатного функціонування.	імовірність	0,7 - 0,99.
Ефективність		
- час відгуку - одержання результатів на типове завдання;	секунди	1 - 1000.
- пропускна здатність - кількість типових завдань, що виконують в одиницю часу.	число у хвилину	1 - 1000.

Виходячи з такого основними функціями, за якими доцільно провести порівняння альтернативних R_1 - R_3 однакового функціонального призначення є (табл.2.8):

функція застосування моделі даних та забезпечення взаємодії ПЕОМ у мережі;

функція реалізації функціональних можливостей ПЗ;

функція забезпечення надійної експлуатації ПЗ.

Таблиця 2.8

Функції ПЗ та можливі варіанти їх реалізації

№ з/п	Функції ПЗ		Варіанти реалізації функцій		
	Назва	Ідентифікатор	Варіант	Назва	Ідентифікатор
1	Застосування моделі даних та забезпечення взаємодії ПЕОМ у мережі	F_1^2	а	застосування об'єктно-реляційної моделі даних	K_1^2
			б	застосування реляційної БД стандартного типу	K_2^2
2	Реалізації функціональних можливостей	F_2^2	а	реалізація процедури оптимізації запитів	K_3^2
			б	реалізація процедури підтримки мережевих протоколів	K_4^2
			в	реалізація процедури розподіленої обробки даних	K_5^2
			г	реалізація процедури зберігання (обробки) мультимедійних і геопросторових даних	K_6^2
			д	реалізація процедури багатомірного аналізу інформації	K_7^2
3	Забезпечення надійної експлуатації	F_3^2	а	забезпечення відновлення після збоїв	K_8^2
			б	забезпечення резервного копіювання та відновлення змін	K_9^2
			в	забезпечення захисту від несанкціонованого доступу	K_{10}^2

Етап 2.

Крок 2.1. Виконаємо процедуру попарного порівняння як самих R_1, R_2 та R_3, так і притаманних ним функцій та варіантів реалізації зазначених функцій (табл.2.12) [32 - 34], використовуючи для цього відомий метод аналізу ієрархій (MAI).

Практика показує, що парні порівняння – найбільш зручна для експертів форма вираження своїх переваг. Можливі ускладнення, яких експерт зазнає при здійсненні парних порівнянь, зводяться до мінімуму, а надмірність інформації, що утримується в заповнених матрицях, дає можливість в процесі наступної обробки значно зменшити вплив помилок експертів при попарному зіставленні цінностей як окремих функцій і критеріїв, так і порівнюваних об'єктів загалом. При здійсненні парних порівнянь функцій і варіантів реалізації зазначених функцій, що характеризують якість ПЗ та власне й самих R_1, R_2 та R_3 за кожним варіантом окремо передбачається, що вони можуть бути задані як якісно, так і кількісно.

За умови, коли відомі кількісні значення варіантів реалізації функцій R_1, R_2 та R_3 (назвемо їх критерії), що обрані для проведення порівняння або висунутих до цих ПЗ технічних вимог (інакше критеріїв порівняння) вихідна матриця матиме вигляд:

$$C = \begin{bmatrix} c_{11} & \dots & c_{1i} & \dots & c_{1N} \\ \dots & \dots & \dots & \dots & \dots \\ c_{j1} & \dots & c_{ji} & \dots & c_{jN} \\ \dots & \dots & \dots & \dots & \dots \\ c_{Q1} & \dots & c_{Qi} & \dots & c_{QN} \\ \dots & \dots & \dots & \dots & \dots \\ c_{R1} & \dots & c_{Ri} & \dots & c_{RN} \end{bmatrix}, \tag{2.14}$$

де c_{ij} - $j-$а варіанти реалізації функцій (стопчики) ПЗ $i-$го типу (рядки).

З метою надання початковим елементам матриці C (2.14) безрозмірного виду проводиться їх нормування за формулою [9 – 11, 14]:

$$B_{ji} = \left[c_{ji} - c_{ji}^{\min}\right] \cdot \left[c_{ji}^{\max} - c_{ji}^{\min}\right]^{-1},\ i = \overline{1, N};\quad j = \overline{1, R}; \tag{2.15}$$

де $c_{ji}^{\min}, c_{ji}^{\max}$ - мінімальне та максимальне значення $j-$го ненормованого значення варіанту реалізації функцій (критеріїв) для ПЗ $i-$го типу.

Коефіцієнти матриць парних порівнянь нормованих значень критеріїв можуть бути обчислені за формулою [35],

$$r_{jk} = B_{ji} / B_{ki}\ ,\ i = \overline{1, N}\ ,\ j = \overline{1, R},\ k = \overline{1, R}\ , \tag{2.16}$$

де B_{ji}, (B_{ki}) - нормовані значення *i-го* критерію j-го, (k-го) ПЗ (R_1, R_2 та R_3).

За інших умов значення функцій та критеріїв можуть бути задані якісно у вигляді показника переваги за вербально-числовою шкалою (табл.2.5 розділу 2.1 даної роботи). Результат порівняння записується при цьому як відношення важливості альтернативи рядка до важливості альтернативи стовпця з обов'язковим урахуванням вимоги взаємної доповненості. Тобто, якщо важливість i-ої функції (критерію, ПЗ) в порівнянні з l-ою дорівнює a_{il}, то важливість l-ої в порівнянні з i-ою дорівнює $a_{li} = 1/a_{il}$. Результат порівняння записується як відношення важливості альтернативи рядка до важливості альтернативи стовпця. Особливу увагу при цьому слід приділяти змісту поставленого запитання. Наприклад: на запитання «Яка з функцій є найбільш визначальною при виборі раціонального ПЗ?» у таблиці першого рівня в чарунці 1,2 (де 1 – номер рядка, 2 – номер стовпця) записується відношення $F_1^2 / F_2^2 = a_{12}$. Якщо F_1^2 має помірну перевагу (невелику) перед F_2^2, записується 3. Якщо F_2^2 має помірну перевагу (невелику) перед F_1^2, то – 1/3. Відповідно в чарунці 2:1 записується зворотне значення

чарунки 1:2, тобто – $1/a_{12}$. При порівнянні однакових альтернатив, наприклад, функції F_1^2 по рядку з функцією F_1^2 по стовпчику, у відповідній чарунці ставиться «1» ($F_1^2/F_1^2=1$). За інших обставин метод аналізу ієрархій, як такий, - не працює.

За умови дотримання зазначених вище вимог будуються обернено симетричні матриці на другому, третьому та четвертому рівнях ієрархії.

Крок 2.2. Визначимо власні вектори та їх нормовані значення для обернено симетричних матриць на другому, третьому та четвертому рівнях ієрархії.

З їх нормованих значень, обчислених за формулою $ABn_{ik}=X_{ik}\Big/\sum_{i=1}^{n}X_{ik}$ ($i=\overline{1,N}$, $k=\overline{1,\text{NTTX}}$), сформуємо узагальнюючу матрицю ABn:

При цьому коефіцієнти відносної злагодженості матриць обчислюються за формулою

$$K_{злаг}^{відн}=\left(I_{злаг}/I_{злаг}^{випад}\right)\cdot 100\%, \qquad (2.17)$$

де $I_{злаг}^{випад}$ - індекс злагодженості матриць, що згенеровані випадковим чином; $I_{злаг}=\left(\lambda_{\max}-N\right)/\left(N-1\right)$ - індекс злагодженості цих матриць; $\lambda_{\max}$ - максимальне власне значення кожної з матриць парних порівнянь; N - кількість порівнюваних елементів (розмірність матриць). Від міри наближення $\lambda_{\max}$ до N залежить ступінь послідовності суджень експертів. Чим вони ближче один до одного, тим результат роботи експертів є більш достовірним. Якщо коефіцієнт відносної злагодженості матриць виходить за межі 10 - 20 %, то експертам потрібно переглянути свої судження та провести другий тур експертизи.

Етап 3.

Крок 3.1. Побудуємо морфологічну карту альтернативних ПЗ (R_1, R_2 та R_3) та визначимо як раціональний варіант реалізації їх основних функцій та/або критеріїв, так й ПЗ ПР в якому цей варіант реалізовано найліпшим чином.

Припустимо, що морфологічна карта альтернативних ПЗ з використанням методу ФВА може мати, наприклад, такий вигляд (рис. 2.8):

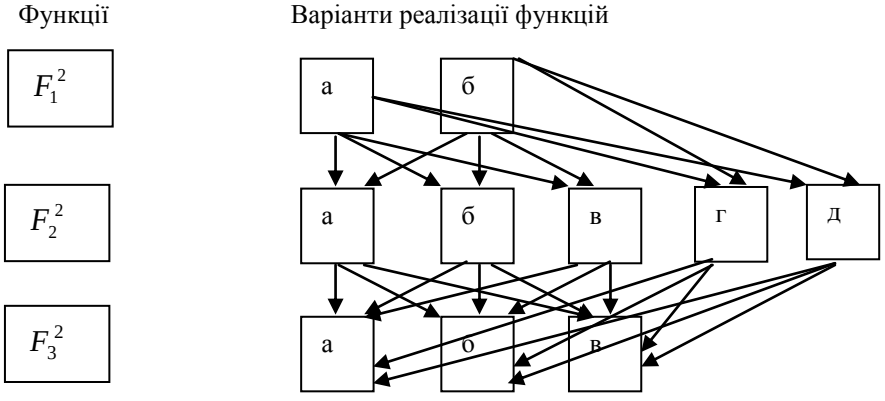


Рис. 2.8. Приклад формування морфологічної карти ПЗ

На основі сформованої морфологічної карти ПЗ побудуємо позитивно-негативну матрицю (ПНМ) варіантів реалізації функцій ПЗ (R_1, R_2 та R_3), обраних для порівняння. Приклад формування ПНМ подано в табл. 2.9 [35].

Ті з варіантів, які мають суттєві недоліки або з різних причин не відповідають умовам технічного завдання (наприклад, у випадку створення СПЗ за замовленням) виключаються з подальшого розгляду. В нашому випадку це варіанти K_2^2, K_3^2, K_6^2, K_7^2 та K_9^2. Інші підлягають техніко-економічному порівняльному оцінюванню.

Таблиця 2.9

Позитивно-негативна матриця варіантів реалізації функцій

Основні функції	Варіанти реалізації функцій	Переваги	Недоліки
F_1^2	а	Простота доступу до інформації, мінімальний час звернення	Дублювання інформації при багатомашинному варіанті
	б	Унікальність інформації, менший об'єм пам'яті	Ускладнення доступу до інформації, збільшення часу звернення
F_2^2	а	Збільшення швидкості обробки інформації	Можливість втрати інформації при збоях
	б	Максимальна наочність інформації, що відображується	Зменшення швидкості обробки інформації
	в	Повне відображення інформації по одному об'єкту	Відсутність інформації по іншим об'єктам
	г	Зменшення імовірності втрати інформації при збоях	Складність реалізації
	д	Можливість порівняння інформації по декількох об'єктах	Часткове відображення інформації
F_3^2	а	Простота і зручність роботи з програмою	Збільшення об'єму програми
	б	Простота і швидкість навчання роботи з програмою	Збільшення об'єму програми
	в	Можливість використання в багатьох програмних комплексах	Збільшення необхідного об'єму оперативнозапам'ятовуючого пристрою

Крок 3.2. Оберемо потенційно можливі варіанти реалізації функцій на підставі їх порівняльного аналізу за перевагами і недоліками (табл. 2.13) та коефіцієнтами вагомості їх критеріїв - φ_k ($k=\overline{1,l}$ та $l=10$), сформованими у виді власного вектору матриці ПП усіх критеріїв K_k^2 між собою, наприклад:

$$1)\ F_1^2 a + F_2^2 б + F_3^2 a;\quad 2)\ F_1^2 a + F_2^2 в + F_3^2 в; \qquad (2.18)$$

$$3)\ F_1^2 a + F_2^2 б + F_3^2 в;\quad 4)\ F_1^2 a + F_2^2 в + F_3^2 a.$$

Крок 3.3. Обчислимо коефіцієнти рівня якості ПЗ ПР (R_1, R_2 та R_3) за кожним критерієм кожної функції

$$K_k^{ПЗ} = \sum_{k=1}^{l} \varphi_k \cdot B_{kj},\quad j=\overline{1,m}\ (m=3) \qquad (2.19)$$

де l – кількість критеріїв конкуруючих ПЗ ПР, які прийняті для оцінювання, $l=10$;

B_{kj} - бальна оцінка k-го критерію j-ї функції якості ПЗ ПР (визначається експертами).

Отримані результати зведемо у таблицю 2.10.

Таблиця 2.10

Розрахунок показників рівня якості варіантів реалізації основних функцій для ПЗ

Функції ПЗ $j=\overline{1,3}$	Критерії ПЗ $k=\overline{1,10}$	Абсолютне значення j-ї функції, A_j	Бальна оцінка k-го критерію j-ї функції B_{kj}	Коефіцієнт вагомості k-го критерію, φ_k	Коефіцієнт рівня якості k-го критерію, $K_k^{ПЗ}$ нормований
F_1^2	а	4	7	0,165	0,114
	б	6,5	2	0,1	0,051
F_2^2	а	16	5	0,174	0,166
	б	0,1	5	0,098	0,091
	в	0,9	9	0,085	0,141
	г	1200	6.5	0,165	0,199
	д	100	4	0,023	0,032
F_3^2	а	1	8	0,034	0,091
	б	0,6	6	0,093	0,097
	в	1	9	0,063	0,018

Кращим варіантом реалізації основних функцій ПЗ з прийнятих для розгляду вважатиметься варіант, якому відповідатиме найбільше значення $K_k^{ПЗ}$:

$$K_{eff} = \max_{1<k<10} K_k^{ПЗ} = K_{ПЗ}^{fynkc}. \qquad (2.20)$$

Таким, наприклад, можу бути варіант г), що відповідає функції F_2^2.

За формулою $K_{ПЗ_j} = K_{kj}^{ПЗ}[F_{1k}] + K_{kj}^{ПЗ}[F_{2k}] + ... + K_{kj}^{ПЗ}[F_{mk}]$, де $j=\overline{1,m}$ (наприклад, $m=3$), $k=\overline{1,l}$ (наприклад, $l=10$) розрахуємо узагальнюючі показники чотирьох варіантів реалізації функцій. Найкращим при цьому вважатиметься варіант, якому відповідатиме найбільше значення відповідного коефіцієнта.

Етап 4. Формування вектору власних значень матриць попарного порівняння критеріїв K_k^2 ($k=\overline{1,l}$, $l=10$) за кожною із функцій F_j^2 ($j=\overline{1,m}, m=10$), тобто їх локальних пріоритетів та матриці $ПЗ_{ik}$, сформованої з власних векторів матриць попарних порівнянь $ПЗ_i$ ($i=\overline{1,n}, n=3$) за кожним із критеріїв K_k^2 ($k=\overline{1,l}, l=10$). Формування власного вектору локальних пріоритетів критеріїв, що використовуються під час порівняння ПЗ ПР - $ХПП_k$.

Етап 5. Обчислення глобальних пріоритетів $ПЗ_i$ ($i=\overline{1,n}$), що дозволять визначити місце кожного з ПЗ ПР серед порівнюваних та визначення їх узагальнених показників якості:

$$ПЗ_i^{glpr} = \sum_{k=1}^{l}(ПЗ_{ik} - ХПП_k)\cdot 100;$$

$$ПЗ_i^{\Sigma} = ПЗ_i^{glpr} \Big/ \min\left(ПЗ^{glpr}\right) \qquad (2.21)$$

Етап 6. З метою урахування суджень потенціальних користувачів щодо важливості критеріїв (ТТХ), які обрані для проведення порівняльного аналізу ПЗ однакового функціонального призначення, при розв'язанні останніми визначених

завдань інформаційної діяльності та підтвердження або спростування рішення, прийнятого на попередньому кроці дослідження, скористаємося формулою:

$$ПЗ_i^{zag} = \sum_{k=1}^{l} (ПЗ_{ik} * bn_k) \cdot 100 \qquad (2.23)$$

де bn_k - вектор вагових коефіцієнтів кожного критерію (ТТХ).

Його середні значення обчислюються за формулою:

$$bn_k := \frac{\sum_{h=1}^{Nekc} Bb_{k,h}}{\sum_{h=1}^{Nekc} \sum_{k=1}^{NTTX} Bb_{k,h}} \qquad (2.24)$$

У цьому випадку $Bb_{k,h}$ - матриця нормованих значень вагових коефіцієнтів критеріїв (наприклад, $NTTX = 10$), визначених у балах в інтервалі від 2 до 5, що надані незалежними користувачами (наприклад, $Nekc = 3$).

За сукупністю функцій і критеріїв, перелічених у табл.2.9 та з врахуванням, як їх важливості на очікуваний результат, так й суджень абонентів щодо їх ваги, кращим серед конкуруючого ПЗ ПР вважатиметься варіант для якого коефіцієнт функціональності $K_{ПЗ}^{fynkc} = \max_{1<j<m} K_{ПЗ_j}$, а коефіцієнт раціональності $K_{ПЗ}^{racion} = \max_{1<i<n} ПЗ_i^{\Sigma}$.

2.4 Процедура вибору типового варіанту побудови перспективної гарантоздатної АСУ ОКІ

Аналіз теорії та практики забезпечення і підтримування необхідного рівня якості при розробці, виробництві та експлуатації АСУ ОКІ дозволив сформувати і узагальнити комплекс протиріч, найбільш значущими серед яких є протиріччя між:

відносно високим рівнем розвитку засобів автоматизації та низьким науково-методичним рівнем досліджень властивостей якості АСУ;

необхідним рівнем продуктивності та обмеженими можливостями промислової бази з виробництва якісної елементної бази і комплектуючих виробів;

закладеним у конструкцію АСУ рівнем відмовостійкості та її необхідним рівнем;

появою нових, більш ефективних АСУ і відставанням у створенні власних подібних систем з необхідним рівнем ефективності;

зростанням витрат на розробку, виробництво та експлуатацію АСУ і реальними економічними можливостями замовника тощо.

Враховуючи таке найбільш ефективним при вирішенні завдання щодо порівняльного аналізу, оцінки якості та вибору раціонального варіанту побудови

перспективної гарантоздатної АСУ ОКІ, як на наш погляд, є так званий «метод Дельфи» [43 – 45]. Його застосування передбачає створення експертної групи, до складу якої доцільно включити представників розробника та Замовника, представників науково-дослідних установ Замовника, а також фахівців-експлуатаційників та кваліфікованих користувачів. Головною мірою стратегії або інакше правилами згідно з якими формуються відповідні рішення та які дають можливість об'єктивно оцінити якість функціонування АСУ при цьому є критерії (властивості):

1) *надійності* (здатність АСУ обраної топології безвідмовно та з досить великою ймовірністю протягом заданого періоду часу виконувати функції при заданих умовах на вихідних даних з області визначення) - $R_1 = K_{MI}^{nad}$;

2) *функціональності* (здатність ПЗ АСУ виконувати набір функцій, що задовольняють заданим або уявним потребам користувачів) - $R_2 = K_{ПЗ}^{fynkc}$;

3) *раціональності ПЗ* (характеризує структуру побудови системи ПЗ АСУ з точки зору її сумісності (здатність включати в себе ОС, програмні засоби і додатки від різних виробників) та продуктивності (здатність працювати якісно у реальному масштабі часу) при вирішенні завдань інформаційної діяльності) - $R_3 = K_{ПЗ}^{racion}$;

4) *ефективності* (відношення рівня послуг, надаваних користувачеві АРМ при заданих умовах, до обсягу використовуваних ресурсів) - $R_4 = K_{APM}^{eff}$.

При цьому кожна властивість може бути охарактеризована додатковими показниками. Як характеристики надійності останнім часом використовують, наприклад, показники:

– безвідмовності (здатність АСУ ОКІ виконувати покладені на неї функції при відмові окремих елементів у заданих умовах функціонування з визначеними показниками якості) такі, як інтенсивність відмов (λ), наробіток на відмову ($T_o^{сист} = 1 \Big/ \sum_{i=1}^{m} \left(C_i / T_{o_i} \right)$) та інші показники. В даному випадку m – кількість елементів, що входять у систему яка розглядається; T_{o_i} – наробіток на відмову i-го елемента системи; C_i – коефіцієнт завантаження i-го елемента системи, $C_i = \overline{0,1}$, $i = \overline{1,N}$;

– довговічності (здатність АСУ ОКІ зберігати в часі працездатний стан без утрати доцільності перебування, наприклад, системи військового призначення на озброєнні до визначених меж такі, як середній або гарантійний термін служби, середній або призначений ресурс тощо;

– ремонтопридатності (здатність АСУ ОКІ до підтримання та відновлення працездатності шляхом технічного обслуговування і ремонту) такі, як, наприклад, середній час, витрачений на відшукання та усунення однієї відмови ($T_в^{сист}$), коефіцієнт готовності системи ($K_г^{сист}$) тощо:

$$T_в^{сист} = \frac{\sum_{i=1}^{m}\left(\left(C_i \cdot T_{в_i}\right)/\left(T_{o_i} + T_{в_i}\right)\right)}{\sum_{i=1}^{m}\left(C_i/\left(T_{o_i} + T_{в_i}\right)\right)} \qquad K_г^{сист} = \frac{1}{\sum_{i=1}^{m}\left(C_i/T_{o_i}\right)\cdot\left(\frac{1}{\sum_{i=1}^{m}\left(C_i/T_{o_i}\right)} + \frac{\sum_{i=1}^{m}\left(\left(C_i \cdot T_{в_i}\right)/\left(T_{o_i} + T_{в_i}\right)\right)}{\sum_{i=1}^{m}\left(C_i/\left(T_{o_i} + T_{в_i}\right)\right)}\right)}$$

де $T_{в_i}$ – середній час відновлення i-го елемента системи.

Для систем, що складаються з елементів, у яких наробіток на відмову багато більше середнього часу відновлення ($T_{o_i} >> T_{в_i}$) вираження для $T_в^{сист}$ й $K_г^{сист}$ значно спрощуються:

$$T_в^{сист} = \sum_{i=1}^{m}\frac{T_o^{сист}\cdot C_i}{T_{o_i}}\cdot T_{в_i}$$

$$K_г^{сист} = \frac{1}{1+\sum_{i=1}^{m}\frac{C_i \cdot T_{в_i}}{T_{o_i}}}$$

Наведені аналітичні вирази можуть використовуватися для систем з будь-яким типом з'єднання елементів [46 - 48]. Оцінка надійності АСУ ОКІ проводиться при цьому в ході проектування та створення системи (апріорна оцінка показників майбутньої системи), при проведенні випробувань, а також в ході експлуатації створеної системи. Показник надійності в даному випадку може бути визначений за допомогою матриці наступного виду:

Класи завдань	Абоненти						
	A_1	A_2	A_3	.....	A_i	.....	A_n
K_1	P_{11}	P_{21}	P_{31}	.....	P_{i1}	.....	P_{n1}
K_2	P_{12}	P_{22}	P_{32}	.....	P_{i2}	.....	P_{n2}
K_3	P_{13}	P_{23}	P_{33}	.....	P_{i3}	.....	P_{n3}
.....	.....	.....	.....	.....	.....	.....	.....
K_j	P_{1j}	P_{2j}	P_{3j}	.....	P_{ij}	.....	P_{nj}
.....	.....	.....	.....	.....	.....	.....	.....
K_l	P_{1l}	P_{2l}	P_{3l}	.....	P_{il}	.....	P_{nl}

де A_1, A_2, A_3, ..., A_i, ..., A_n – користувачі або абоненти АСУ; n – кількість користувачів (абонентів) у системі; l – кількість розв'язуваних класів завдань; K_1, K_2, K_3, ..., K_j, ..., K_l – різні класи розв'язуваних завдань; P_{ij} – обрана сукупність показників надійності системи для i-го абонента при вирішенні j-го класу завдань.

У рядках матриці надійність системи визначена багатозначністю першого порядку, а в стовпцях – багатозначністю другого порядку. В окремих випадках вона може істотно спрощуватися. Наприклад, коли всі завдання, розв'язувані користувачами, можна віднести до одного класу, вся матриця зведеться до одного рядка. Для АСУ, що мають абонентів з ідентичними структурними схемами надійності системи [6, 7], коли має сенс говорити про надійність для типів абонентів, матриця також матиме спрощений вигляд.

Описуючи залежність надійності системи від характеристик елементів, що входять до її складу, вони визначають неоднозначність значень показників надійності для різних режимів роботи системи основними з яких, наприклад, при роботі з інформацією є: підготовка вихідної інформації та подання її у придатному для формування запиту виді; введення запиту та пошук відповіді на нього; видача відповіді на оброблений запит; сприйняття та обробка відповіді на запит. Виходячи з цього надійність функціонування АСУ ОКІ (H) може бути визначена за формулою:

$$H = \prod_{i=1}^{5}(1 - Q_i), \tag{2.25}$$

де Q_i – імовірність появи помилки на одному з наведених вище режимів.

Загальний позитивний стан надійності АСУ може бути охарактеризований, наприклад, таким чином: трафік по мережевій службі системи передається надійно з гарантованим захистом як від вірусів, так й від атак порушників; широкий спектр послуг надається системою безперебійно за гнучкою схемою 24х7, тобто 24 години на добу протягом 7 днів тижня.

Алгоритм застосування методу Дельфи для вибору типового варіанту побудови перспективної гарантоздатної АСУ ОКІ (рис.2.9) являє собою систематизовану послідовність кроків, що подані нижче [49].

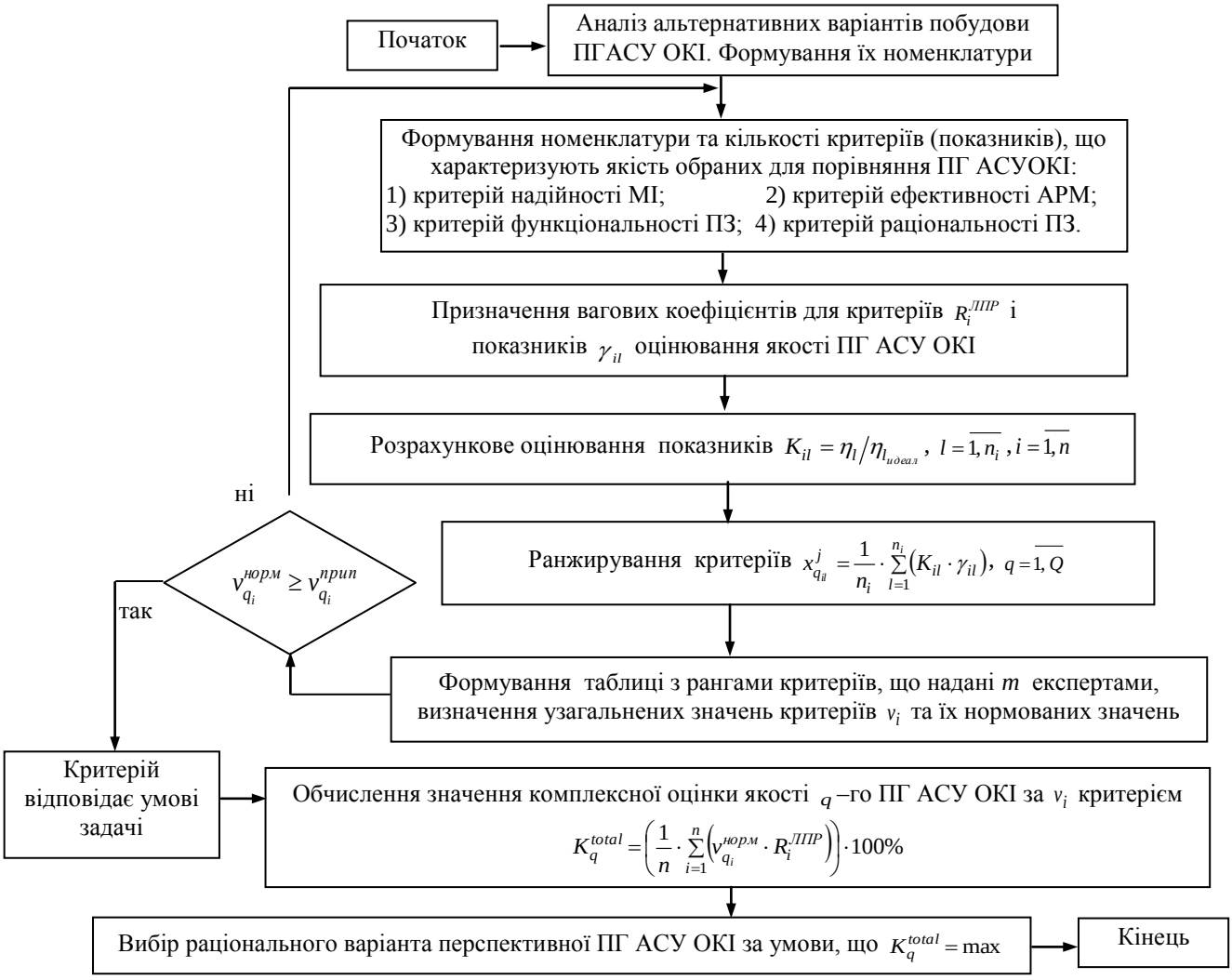


Рис. 2.9. Структурно-логічна схема алгоритму вибору типового варіанту побудови ПГ АСУ ОКІ

Етап 1. Структурування проблеми вибору раціонального варіанту для створення перспективної гарантоздатної АСУ ОКІ у вигляді ієрархії та виявлення її найбільш важливих елементів, а саме множин (табл.2.11):

критеріїв R_j ($j=\overline{1,m}$, $m=4$) щодо надійності МІ (K_{MI}^{nad}), ефективності АРМ (K_{APM}^{eff}), функціональності ($K_{ПЗ}^{fynkc}$) та раціональності ($K_{ПЗ}^{racion}$) ПЗ серед яких необхідно вибрати найкращий;

показників Y_i, де $i=\overline{1,n}$, $n=12$, що характеризуватимуть критерій Y_j (готовності, безперебійності, відновлюваності, доступності, змінюваності, змінюваності, вивчає мості, адаптованості, простоти інсталяції, відкритості, забезпечення єдиного ТК простору та захищеності).

Таблиця 2.11

Оцінка критеріїв і показників якості АСУ, що може бути сформована з використанням результатів попередніх досліджень

Критерій оцінки АСУ	**Вага критерію оцінки R_i**	**Показник критерію**		
		Функція, що притаманна показнику	**Міра виміру**	**Шкала виміру**
Надійність магістраль маг МІ	K_{MI}^{nad} = 3.864	***Готовність:*** готовність до роботи обл..лінійного тракту	імовірність	0.1-0.99
		Безперебійність: середній час між відмовами	год.	200-5000
		Відновлюваність: середній час відновлення	год.	2-100
Функціональність ПЗ	$K_{ПЗ}^{fynkc}$ =0.346	***Доступність***: відносний час пра цездатного функціонування	імовірність	0.1-0.99
		Змінюваність: тривалість підготовки змін	год.	1-1000
		Замінюваність: тривалість заміни компонентів ПЗ	год.	1-100
Раціональність ПЗ	$K_{ПЗ}^{racion}$ =1.175	***Вивчаємість***: трудомісткість вивчення і застос.ПЗ	чол/год.	1-1000
		Адаптованість: трудомісткість адаптації	чол/год.	1-100
		Простота установки: тривалість інсталяції ПЗ	чол/год.	1-100
Ефективність АРМ	K_{APM}^{eff} =0,9	***Відкритість:*** можливість роботи у складі АСУ	порядкова	1-10
		Забезпечення єдиного ТК простору: внутрішньо системна інформаційна звя'зність	порядкова	1-10
		Захищеність: багаторівнева система захисту даних	порядкова	1-10

Примітка: Кількість показників якості, що перебувають на одному рівні ієрархії, з врахуванням психофізичної гіпотези Міллса не повинна перевищувати при цьому $7 \div 9$. Людина не може одночасно порівнювати більше ніж $\lhd 7+2 \rhd$ об'єктів.

Експерти разом із Замовником призначають вагові коефіцієнти важливості для γ_{il} - *l-го* показника *i-го* критерію. Для цього вони використовують наступну шкалу:

5 – досить важливо, щоб даний показник мав високе значення;

4 – важливо, щоб даний показник мав високе значення;

3 – добре б мати високе значення даного показника;

2 – корисно мати високе значення даного показника;

1 – відчутних втрат не передбачається, - виходячи при цьому з того, що вага найменш відповідального критерію (властивості) має дорівнювати одиниці.

Етап 2. Експерти оцінюють *l-й* показник *i-го* критерію (властивості) - K_{il}^{j} з погляду повноти реалізації властивої йому функції за формулою:

$$K_{il}^{j} = \frac{\eta_l}{\eta_{l_{идеал}}},\ i = \overline{1,n},\ l = \overline{1,n_i},\ j = \overline{1,m},\ K_{il}^{j} \in [0,1]. \qquad (2.26)$$

де η_l – рахункова кількість одиниць *l-го* показника *i-го* критерію (властивості), що характеризують повноту реалізації тієї або іншої функції; $\eta_{l_{идеал}}$ – ідеальна кількість таких одиниць (повинна бути визначена в технічних умовах на створення АСУ та відповідному технічному завданні); n – кількість критеріїв; n_i – кількість показників *i-го* критерію (властивості). m – кількість задіяних в роботі експертів.

Таким чином, обрані критерії (властивості) оцінювання АСУ ОКІ можуть бути виражені через чисельні показники.

Етап 3. Експерти проводять комплексну оцінку *i-го* критерію. При цьому $x_{q_{il}}^{j}$ - ранг *i-го* критерію (властивості) по альтернативному рішенню q, приписуваний j-м експертом обчислюється за формулою:

$$x_{q_{il}}^{j} = \frac{1}{n_i} \cdot \sum_{l=1}^{n_i} (K_{il} \cdot \gamma_{il}),\ q = \overline{1,Q}, \qquad (2.27)$$

де K_{il} – експертна оцінка *l-го* показника *i-го* критерію (властивості);

γ_{il} – ваговий коефіцієнт важливості *l-го* показника *i-го* критерію (властивості);

Q – загальна кількість АСУ, що підлягають оцінюванню.

Етап 4. Експертами проводяться заходи щодо:

по-перше, формування узагальненої таблиці з комплексних оцінок *i-х* критеріїв (властивостей) для досліджуваної АСУ підтримки прийняття управлінських рішень, отриманих ними в ході виконання попередніх етапів роботи;

по-друге, сумарного ранжирування за альтернативним рішенням q:

$$\sum_{j=1}^{m} x_{q_1}^{j},\quad \sum_{j=1}^{m} x_{q_2}^{j},\quad .... \qquad (2.28)$$

де x – ранг *i-го* критерію по альтернативному рішенню q (в даному випадку $q = 1$), приписуваного j-м експертом; m – кількість задіяних в роботі експертів.

по-третє, визначення коефіцієнта згоди W_q між існуючими думками фахівців за формулою [47, 48]:

$$W_q = \frac{\sum_{i=1}^{n} \left\{ \sum_{j=1}^{m} \left(x_{q_i}^{j} \right) - \frac{1}{2} \cdot m \cdot (n+1) \right\}^2}{\frac{1}{12} \cdot m^2 \cdot \left(n^3 - n \right) + m \cdot \frac{1}{12} \cdot \sum_{t_j} \left(t_j^3 - t_j \right)} \qquad (2.29)$$

де t_j - число повторень кожного рангу в ранжируванні, що надане j-м експертом.

Якщо $W_q = 0$, то погоджена точка зору фахівців з даного ранжирування відсутня.

Якщо $W_q = 1$ - погодженість думок повна. Для оцінювання значимості результатів при $n \le 7$ варто використати розподіли Фішера, при $n > 7$ - розподіл χ^2.

Припустимо, що в ході оцінювання довільної АСУ m експертами була сформована наступна таблиця даних (табл. 2.12). Їх значення округлені до цілого:

Таблиця 2.12

Узагальнені результати

№ експерта	**Критерій (властивість)** $x^j_{q_{il}}$			
	Надійність МІ	**Функціональність ПЗ**	**Раціональність ПЗ**	**Ефективність АРМ**
1	1	2	4	3
2	2	3	1	4
3	3	2	1	4
4	1	2	3	4
5	1	3	4	2
6	1	2	3	4
7	1	2	4	3
8	2	3	1	4
9	3	4	2	1
10	1	2	4	3
Сумарні ранги критеріїв x_Σ	**16**	**25**	**27**	**32**
Ранжирування критеріїв	**1**	**2**	**3**	**4**

Виходячи зі значень, наведених у таблиці 2.22, коефіцієнт згоди, розрахований за формулою (4.5) буде дорівнювати:

$$W_q = \frac{\sum_{i=1}^{4}\left\{\sum_{j=1}^{10}\left(x^j_{q_i}\right) - \frac{1}{2}\cdot 10\cdot(4+1)\right\}^2}{\frac{1}{12}\cdot 10^2\cdot\left(4^3-4\right)} \approx 0.268\cdot$$

Застосувавши для оцінки значимості отриманого результату статистичні таблиці розподілу Фішера для $n = 4$ й $W_q = 0.268$ можна зробити висновок, що погодженість між думками експертів існує з імовірністю ≈ 0.99.

Представивши результати таблиці 2.22 (сумарні ранги критеріїв (властивостей)) у вигляді вектора-рядка: $x_\Sigma = \left\| x^j_{q_{il}} \right\| = \|16 \quad 25 \quad 27 \quad 32\|$

і позначивши вагу найбільш відповідального критерію (властивості) через $v_1 = 2$, а найменш відповідального критерію (властивості) через $v_4 = 1$ по формулі [49]:

$$v_q = v_4 + \frac{y_q - y_4}{y_1 - y_4}\cdot(v_1 - v_4) \qquad (2.30)$$

знайдемо ваги інших критеріїв (властивостей), де:

$y_1 = 16$ - сумарний ранг найбільш відповідального критерію;

$y_4 = 32$ - сумарний ранг найменш відповідального критерію.

Після обчислень отримаємо: $v_2 = 1.44$, $v_3 = 1.31$.

Провівши нормування розрахованих ваг критеріїв (властивостей) - v_1, v_2, v_3 і v_4 за формулою $v_i^{нор} = v_i \Big/ \sum_{i=1}^{n} v_i$ $(n = 4)$, сформуємо таблицю 2.13.

Таблиця 2.13

Нормовані ваги критеріїв (властивостей)

	Критерій (властивість)			
	Надійність МІ	**Функціональність ПЗ**	**Раціональність ПЗ**	**Ефективність АРМ**
Нормована вага критерію (властивості) $v_q^{норм}$	0.347	0.250	0.227	0.176

Для збільшення коефіцієнта згоди W_q по ранжируванню пропонованих критеріїв (властивостей) можливо по черзі виключати одного або декількох експертів [44]. Виключається або ж пояснює свій підхід до ранжирування критеріїв (властивостей), як правило, експерт, думка якого найбільше впливає на загальний коефіцієнт згоди інших фахівців. Після цього по формулах (2.27) – (2.30) визначається значення комплексної оцінки *і-го* критерію (властивості), а по формулі (2.31) – їхня вага. Остаточне нормування ваг досліджуваних критеріїв (властивостей), що характеризують конкретну АСУ, визначається для максимального коефіцієнта згоди.

Якщо роль m експертів виконує лише особа, уповноважена приймати рішення (ОПР), то сумарні ранги критеріїв (властивостей) згідно даних таблиці 2.14 матимуть вид: $x_{\Sigma} = \left\| x_{q_{il}}^{j} \right\| = \|3{,}53 \quad 1{,}36 \quad 1{,}65 \quad 2{,}91\|$.

Тоді, позначивши:

1) вагу найбільш відповідального критерію (властивості) через $v_1 = 2$, а найменш відповідального критерію (властивості) через $v_2 = 1$;

2) сумарний ранг найбільш відповідального критерію через $y_1 = 1{,}36$, сумарний ранг найменш відповідального критерію $y_2 = 3{,}53$

за формулою $v_q = v_2 + \dfrac{y_q - y_2}{y_1 - y_2} \cdot (v_1 - v_2)$, отримаємо:

Таблиця 2.14

Реальні та нормовані ваги критеріїв (властивостей) АСУ
за умови 1 безальтернативого варіанту побудови та прийняття рішення ОПР

	Критерій (властивість)			
	Надійність МІ	**Функціональність ПЗ**	**Раціональність ПЗ**	**Ефективність АРМ**
Реальна вага критерію (властивості)	1,000	2,000	1,867	1,286
Нормована вага критерію (властивості) $v_q^{норм}$	0.163	0.325	0.303	0.209
Ранжирування критеріїв	**4**	**1**	**2**	**3**

Етап 5. Особа, що уповноважена приймати рішення (ОПР) проводить порівняння нормованої величини значення, що прийняв певний крітерій (властивість) з припустимими значеннями, визначеними у технічних умовах на створення АСУ та відповідному технічному завданні. При виконанні умови критерій (властивість) позначається як такий, що позитивно пройшов випробування.

Етап 6. ОПР обчислює [49] комплексний показник якості досліджуваної АСУ K_q^{total} за кожним q-м альтернативним рішенням побудови АСУ за формулою:

$$K_q^{total} = \left(\frac{1}{n} \cdot \sum_{i=1}^{n} \left(v_{q_i}^{норм} \cdot R_i^{ОПР} \right) \right) \cdot 100\% \qquad (2.31)$$

де $v_{q_i}^{норм}$ – нормована вага *i-го* критерію (властивості);

$R_i^{ОПР}$ – середнє значення вагового коефіцієнта важливості кожного критерію (властивості), визначене m незалежними експертами: $R_i^{ОПР} = \sum_{j=1}^{m} R_{ij}^{нор} \Big/ \sum_{j=1}^{m} \sum_{i=1}^{n} R_{ij}^{нор}$;

$R_{ij}^{нор}$ - нормована вага *i-го* критерію (властивості) за q-м альтернативним рішенням побудови АСУ, приписувана j-м експертом $R_{ij}^{нор} = R_{ij} \Big/ \sum_{i=1}^{n} R_{ij}$. Для визначення вагового коефіцієнта $R_{ij}^{ОПР}$ кожного з критеріїв (властивостей) використовуються дані з матриці вагових коефіцієнтів, складеної на основі думок експертів за результатами заповнення таблиці-анкети (табл. 4.2):

$$\begin{vmatrix} R_{11} & \dots & R_{1j} & \dots & R_{1m} \\ \dots & \dots & \dots & \dots & \dots \\ R_{i1} & \dots & R_{ij} & \dots & R_{im} \\ \dots & \dots & \dots & \dots & \dots \\ R_{n1} & \dots & R_{nj} & \dots & R_{nm} \end{vmatrix}, i = \overline{1,n} \ , \ j = \overline{1,m},$$

де n – кількість критеріїв (властивостей); m – кількість задіяних в роботі експертів.

Якщо розгляду підлягає q альтернативних рішень побудови АСУ, то остаточний вибір серед них раціонального варіанта буде здійснюватися на підставі наступного правила: якщо $K_q^{total} \geq K_{q+1}^{total}$, то q-й варіант АСУ є більше якісним у порівнянні з $q+1$ та навпаки; якщо $K_q^{total} = K_{q+1}^{total}$, то варіанти рівнозначні. За раціональний серед порівнюваних альтернативних варіантів побудови АСУ ОКІ або ж у випадку безальтернативного дослідження ОПР обирає той варіант АСУ, якому відповідає $K_q^{total} = \max$ [49].

Застосування методу дасть ОПР інструмент для визначення рівня впливу кожного критерію на якість функціонування ПГ АСУ ОКІ, обчислювати комплексні

показники якості її конкуруючих варіантів та здійснювати їх порівняльний аналіз, оцінювати чутливість комплексних показників якості при зміні міркувань учасників експертної групи тощо. На підставі отриманих результатів особа, що приймає рішення зможе серед деякого розмаїття альтернативних рішень обрати раціональний з точки зору якості варіант побудови перспективного СПАККР та сформувати рекомендації з підвищення ефективності, продуктивності і надійності його застосування.

Висновки до другого розділу

АСУ ОКІ, як один із вузлів найпоширенішої на сьогодні технології Internet, може бути орієнтований або на вирішення певних завдань інформаційно-аналітичної дяльності, або ж на забезпечення виконання певних технологічних процесів. Зважаючи на таке, при проектуванні та створенні перспективної гарантоздатної АСУ ОКІ, доцільно визначитись як з прототипом топології мережі, так і з тим добором програмно-апаратних засобів, які забезпечуватимуть її функціонування. При цьому саме топологія мережевої інфраструктури перспективної гарантоздатної АСУ ОКІ, яка визначає конфігурацію мережі у цілому, є одною з найважливіших її характеристик.

Прийняття рішення щодо вибору серед існуючих топологій сучасних КМ прототипу для створення мережевої інфраструктури перспективної гарантоздатної АСУ ОКІ є, як правило, наслідком деякого компромісного рішення за критеріями вартості, функціональності та відповідності технічним вимогам стосовно кожної конкретної ситуації. Головними характеристиками, які впливають на вибір прототипу топології серед існуючого їх розмаїття є показники, що певним чином характеризують програмно-апаратні засоби та використовуваний інтерфейс з точки зору:

ціни, проведення монтажних робіт, робіт з обслуговування, тощо;

діагностування, масштабованості, гнучкості та універсальності, тощо;

швидкості роботи, захищеності від відмов, тощо.

Грунтуючись на зазначених критеріях і показниках в роботі вибір прототипу топології МІ серед низки можливих пропонується здійснювати за глобальним пріоритетом досліджуваних топологій - AB_{glpr}.

Для гарантування точності і вірогідності інформаційного забезпечення, яке є неодмінним фактором надійного і ефективного функціонування АСУ ОКІ застосовуються автоматизовані робочі місця користувачів – керівників та виконавців. Вони створюються на базі персональних комп’ютерів (ПЕОМ), типового або спеціалізованого периферійного обладнання, а також відповідного

програмного забезпечення. Застосування запропонованої в роботі процедури вибору типового АРМ раціональної конфігурації дозволяє за безрозмірним розрахунковим показником максимальної продуктивності $P_{prodykt}^{\max}$ з декількох альтернативних пропозицій, призначених для вирішення завдань інформаційної діяльності, обрати раціональний варіант, який функціонуватиме у єдиному інформаційно-телекомунікаційному просторі та відповідатиме вимогам відкритості, захищеності, якості, надійності та ефективності функціонування, а також компактності розміщення, легкості налаштовування, простоті експлуатації та поетапності впровадження.

Зважаючи на те, що автоматизація всіх процесів діяльності АСУ ОКІ та АРМ зокрема потребує формування системи їх раціонального ПЗ, запропонований в роботі метод дозволяє враховувати якісні характеристики в корисності ПЗ однакового функціонального призначення, а саме головні функції (критерії) та множинність цілей ПЗ та можливий ефект від їх взаємодії, а також упорядковувати альтернативні варіанти та за одержаними ваговими коефіцієнтами визначати їх місце в загальному переліку ПЗ, що порівнюються. Обґрунтоване рішення щодо формування в інтересах створення перспективної АСУ системи раціонального ПЗ ґрунтується при цьому на безрозмірних розрахункових показниках функціональності $K_{ПЗ}^{fynnkc}$ та раціональності ПЗ $K_{ПЗ}^{racion}$.

Визначитись з тим, який варіант побудови перспективної гарантоздатної АСУ ОКІ набагато якісніший за аналогічні конкурентоспроможні варіанти допоможе метод, в якому вибір раціонального варіанту побудови здійснюється за допомогою комплексного безрозмірного показника K_q^{total}. Кращим за інші з точки зору топології мережевої інфраструктури АСУ, її архітектури (зокрема АРМ) та програмного забезпечення, а також властивих для неї функцій вважатиметься той варіант, для якого $K_q^{total} = \max$.

В перспективі представлений у розділі науково-методичний апарат може бути використаним при створенні автоматизованих систем, спрямованих на забезпечення вирішення завдань інформаційної та інформаційно-аналітичної діяльності спеціалізованими підрозділами будь-якого підпорядкування. Результати його апробації були отримані завдяки застосуванню універсальної системи математичних розрахунків «MATHCAD». Лістінг підпрограм проведення досліджень наведений у Додатках Б та В.

Список джерел, використаних у другому розділі

1. ДСТУ 2226-93 Автоматизовані системи. Терміни і визначення.
2. Гук М. Аппаратные средства локальных сетей. Энциклопедия. – СПб.: Питер, 2000. – 576 с., ил.
3. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 2-е изд. – СПб.: ПИТЕР, 2003. – 864 с.
4. Рейш О.Е., Бурячок В.Л., Вертегел С.Г., **Бурячок Л.В.** Методика вибору раціональної топології комп'ютерної мережі перспективних автоматизованих систем управління військами. Труди Академії. – К.: НАО МО України, 2009. – № 2(89). – С. 81–90.
5. Буров Є. Комп'ютерні мережі. 2-ге оновлене і доповн. вид. – Львів: БаК, 2003. – 584 с.
6. Семенов А.Б., Стрижаков С.К., Сунчелей И.Р. Структурированные кабельные системы. 5-е изд., перераб. и доп.– М.: ДМК-Пресс, 2004, – 640 с.
7. Антонов В.М. Сучасні комп'ютерні мережі. – Київ: МК-Прес, 2005. – 480 с.
8. Бурячок В.Л. Технологія прийняття рішень у складних соціотехнічних системах: Монографія. / В.Л. Бурячок, В.О. Хорошко. / Під заг. ред. докт. техн. наук, проф.В.О. Хорошка. – К.:ДУІКТ, 2012. – 344 с.
9. Брахман Т.Р. Многокритериальность и выбор альтернативы в технике. – М.: Радио и связь, 1984. – 288 с.
10. Васильев Ю.Л. Спектральный подход к сравнению обьектов, охарактеризованных набором признаков. ДАН СССР, сер. "Математика. Физика.", т. 206, №6. – М.: 1972
11. Черноскутов А.И., Мурзин В.Н. Комплексная оценка качества изделий с помощью метода прогрессирующего эталона //Надежность и контроль качества №4, 1985
12. Статистические методы в инженерных исследованиях: Учебное пособие /Под ред. Г.К.Круга. – М.: Высш. школа, 1983. – 216 с.
13. Бек Н.Н., Голенко Д.И. Статистические методы оптимизации в экономических исследованиях. – М.: Статистика, 1971. – 136 с.
14. Кини Р.Л., Райфа Х. "Принятие решений при многих критериях: предпочтения и замещения: Пер. с англ. /Под ред И.Ф.Шахнова,-М.Радио и связь. 1981. – 560с.
15. Теория выбора и принятия решений: Учебное пособие. –М.: Наука. Главная редакция физико-математической литературы, 1982. – 328 с.
16. Саати Т. Принятие решений: метод анализа иерархий. //Пер с англ. – М.: радио и связь, 1993. – 240 с.
17. Dreis Y. A tuple model for estimating the consequences of personal data leakage in automated systems. VIII International conferece of students, PHD-students and young

scientists «Engineer of XXI Century» /Y.Dreis, I.Lozova, A.Biskupskyi, **L.Kuzmenko**, Ali .T. Al-Khwalde, A.Korchenko // Processing, transmission and security of information. – Bielsku-Białej: NATH, 2018. Vol.2. – P. 41–50. ISBN: 978-83-65182-94-4.

18 Бурячок В.Л., **Бурячок Л.В.** Поняття кібервійни та розвідки інформаційно-телекомунікаційних систем у контексті захисту держави від стороннього кібернетичного впливу. Вісник воєнної розвідки. – № 26. – 2012. – С. 45–52.

19. Бурячок В.Л., **Бурячок Л.В.,** Кураев К.А. Показники та критерії надійності функціонування інформаційно-телекомунікаційних систем спеціального призначення. – К.: НДІ ГУР МО України, 2014. Вип. 38. – С. 34–47.

20. Feodosiy Kipchuk, Volodymyr Sokolov, Volodymyr Buriachok, Pavlo Skladannyi, **Lidiia Kuzmenko**. Investigation of Availability of Wireless Access Points based on Embedded Systems. Proceedings of the VI International Scientific and Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T'2019), October 8–11, 2019: abstracts. — Kyiv : IEEE, 2019. — P. 246–250 (*Цитування в Scopus*)

21. Політика інформаційної безпеки: підручник. / В. Л. Бурячок, Р. В. Грищук, В. О. Хорошко /. За заг. ред. докт. техн. наук, проф. В.О. Хорошка. – К. : ПВП «Задруга», 2014. – 222 с.

22. Степанова Е.Е. Информационное обеспечение управленческой деятельности. / Е.Е.Степанова, Н.В.Хмелевская. – М.: Инфра-М, 2002. – 154 с.

23. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. – К. : ДУТ, 2015. – 345 с

24. Воройский Ф.С. Проектирование информационной технологии и автоматизированных рабочих мест в составе служб предприятия: Нормативные и методические материалы. Организация информационной деятельности / Ф.С. Воройский, С.В. Моздор. – М.: ВИМИ, 2002. – 75 с.

25. С.В.Бушуев, Б.В.Рожкин «Требования к АРМАМ и тенденции их развития в составе систем управления технологическими процессами». [Электронный ресурс] Режим доступа к статье: http://nilksa.ru/content_files/research113.pdf

26. А.П.Кохан «Эффективность автоматизированного робочого места: критерии оценки и методы повышения». [Электронный ресурс] Режим доступа к статье: http://www.belisa.org.by/pdf/PTS2005/213-218.pdf

27. Дорофеев Р.А. Совершенствование финансово-экономической деятельности соединения в условиях внедрения новых информационных технологий. [Электронный ресурс] Режим доступа к статье: http://works.tarefer.ru/99/100822/index.html

28. Бурячок В.Л., **Бурячок Л.В.,** Гулак Г.М. Алгоритм вибору АРМ раціональної конфігурації. Сучасний захист інформації. – К.: ДУІКТ, 2011. – № 2. – С. 85–94.
29. V. Lakhno, V. Malyukov, N. Mazur, **L. Kuzmenko,** B. Akhmetov. Development of a model for decision support systems for managing the process of investing in information technology. Східно-Європейський журнал передових технологій. ТОМ 1, № 3 (103) (2020), с. 74 – 81. ISSN (print) 1729-3774, ISSN (on-line) 1729-4061 (*Цитування в Scopus*)
29. Соммервилл И. Инженерия программного обеспечения ; [пер. з англ.] – М. : Издательский дом "Вильямс", 2002. – 624 с.
30. Програмні засоби ЕОМ. Показники та методи оцінювання якості : ДСТУ 2850–94.. – [Чинний від 01.01.96.] – К.: Дежстандарт України, 1994. – 20 с.
31. Информационные технологии. Оценка продукции программного обеспечения. Характеристика качества и руководящие положения по их применению : ГОСТ Р ИСО/МЭК 9126-93.
32. Тоценко В. Г. Методы и системы поддержки принятия решений. /В. Г. Тоценко. – К.: Наук. думка, 2002. –381 с.
33. Чумаков Н.М. Оценка эффективности сложных технических устройств /Н.М.Чумаков, Е.Н.Серебрянный. – М.: Сов. радио, 1980. – 192 с.
34. Бурячок В.Л., **Бурячок Л.В.** Алгоритм порівняльного оцінювання програмних засобів однакового функціонального призначення для розв'язання завдань інформаційної діяльності. Збірник наукових праць. – К.: НДІ ГУР МО України, 2010. Вип. 27. – С. 124–139.
35. Брахман Т.Р. Многокритериальность и выбор альтернативы в технике. /Т.Р.Брахман. – М.: Радио и связь, 1984. – 288 с.
36. Бурячок В.Л., **Бурячок Л.В.,** Костюк Т.Я. Формування набору показників для оцінювання якості програмного забезпечення сучасних автоматизованих систем. Збірник наукових праць. – К.: НДІ ГУР МО України, 2010. Вип. 28. – С. 111–124.
37. Бурячок В.Л., **Бурячок Л.В.,** Костюк Т.Я. Обґрунтування вибору раціональної системи електронного документообігу для державних структур спеціального призначення. Вісник воєнної розвідки. – № 24. – 2011. – С. 67–74.
38. Грабовский М. Современные технологии и стандарты разработки программного обеспечения // Корпоративные системы. – 2000. – № 1. – С. 75-80.
39. **Бурячок Л.В.** Стратегія обґрунтування раціонального набору параметрів і функцій програмних засобів спеціального призначення, спрямованих на розв'язання завдань інформаційної діяльності. Сучасний захист інформації. – К.: ДУТ, 2016. – № 3. – С. 3–9.

40. Бурячок В.Л., **Бурячок Л.В.,** Боголій С.М. Порівняльне оцінювання програмних засобів однакового функціонального призначення. «Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення». V-а НТК ВІТІ НТУУ "КПІ" МО України, 20–21.10.2010 р.. Доповіді та тези доповідей. – К.: ВІТІ НТУУ "КПІ", 2010. – С. 75–76.

43. Кендал М. Ранговые корреляции. /Пер. с англ. – М.: Статистика, 1975. – 213 с.

44. Добров Г.И., Ершов Ю.А., Левин Е.И., Смирнов Л.П. Экспертные оценки в научно-техническом прогнозировании /Под общ. ред. В.С. Михалевича. – Киев: Наукова думка 1974. – 160 с.

45. Дэвид Г. Метод парных сравнений /Пер. с англ. – М.: Статистика, 1976. – 568 с.

46. Бешелев С. Д., Гурвич Ф. Г. Экспертные оценки. – М.: Наука, 1973. – 263 с.

47. Осипов Н.В., Нечаев А.Н. и др. Методика статистической обработки коллективных экспертных оценок. Деп.. в УкрНИИНТИ 20.0985, № 2247. Библ. Ук. ВИНИТИ № 1 (171), 1986. б/о 1362.

48. Чирков В.Г. Выбор рациональных технических решений. – К.: Техника, 1991. –159 с. (Б-ка инженера).

49. **Бурячок Л.В.,** Бурячок В.Л., Семко В.В. Технологія проведення порівняльного аналізу та оцінювання стану захищеності автоматизованих інформаційних систем. Сучасний захист інформації. – К.: ДУТ, 2016. – № 4. – С. 16–24.

Розділ 3
МЕТОД ВИЗНАЧЕННЯ ВПЛИВУ ЗАГРОЗ НА ПРОЦЕСИ ФУНКЦІОНУВАННЯ ПЕРСПЕКТИВНОЇ ГАРАНТОЗДАТНОЇ АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ ОБ'ЄКТАМИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

У питаннях створення інформаційних систем ОКІ, організації та забезпечення їх захисту від стороннього кібернетичного впливу з точки зору сторони, що убезпечує власний ресур доволі часто постають питання [1 – 3]:

1) що саме захищати, від кого захищати та яким чином захищати;

2) що є об'єктом, а хто є суб'єктом захисту;

3) як забезпечити надійний захист інформації від сторонніх осіб шляхом її криптографічних перетворень;

4) як відновити зашифровані дані за оперативно придатний час;

5) яка із можливих систем захисту є найбільш надійною та не дозволить атакуючій стороні подолати захисні бар'єри, тощо.

Виходячи з цього можуть суттєво відрізнятися як послуги безпеки, які надаватимуться певним об'єктам або суб'єктам захисту та механізми безпеки АСУ ОКІ, завдяки яким ці послуги можуть бути реалізовані (рис.3.1).

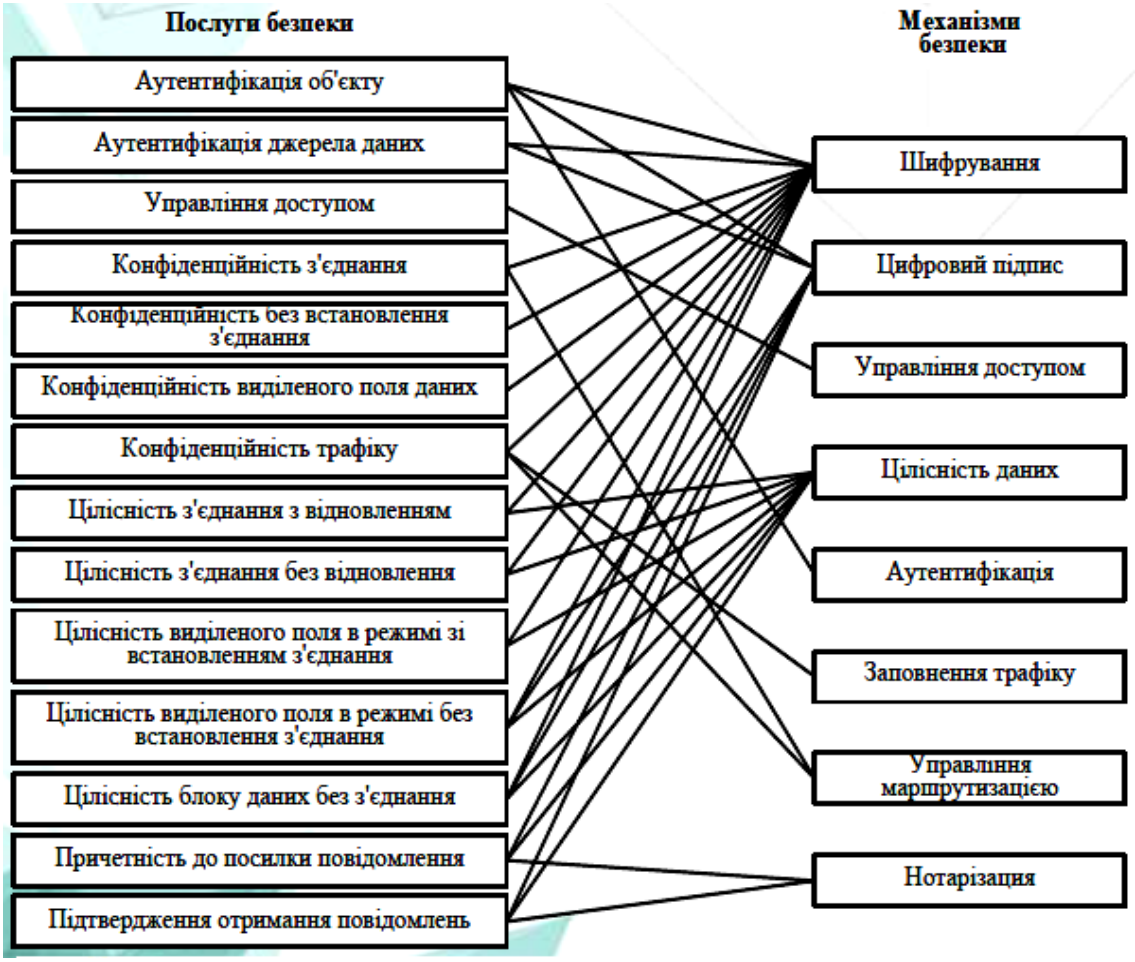


Рис.3.1 Механізми і послуги безпеки

Об’єктом захисту при цьому може бути як інформація (інформаційні ресурси) та/або інформаційна система ОКІ (системи і канали зв'язку, канали передачі даних, АРМ, аккаунти, сервіси, хости, мережа, мережеві служби), де ІР циркулюють, обробляються і накопичуються тобто знаходяться у взаємодії з інформаційним середовищем, а також з використанням ресурсів якої передаються, так й інформаційні та технологічні процеси, що протікають на об’єкті із застосуванням ІС. Суб’єктом захисту – як власник інформації, ІС, технологій та засобів їх забезпечення, так й користувач, який звертається до ІС та користується необхідною йому інформацією.

Традиційний підхід до організації і забезпечення захисту АСУ ОКІ [2] ґрунтується на тому, що клієнт (користувач, власник) застосовуючи міжмережеві екрани та систему паролів, біометричні системи ідентифікації та RAID-масиви, антивірусні програми, тощо робить все сам: захищає дані (інформацію, ІР) і кінцеві пристрої; проводить ідентифікацію, автентифікацію та авторизацію; здійснює захист комунікацій та периметру (рис. 3.2).

Рис.3.2 Механізми і послуги безпеки

Застосовуючи більш спеціалізований підхід до виконання процедур, зазначених вище, клієнт (власник) користується послугами команди професіоналів, яка в комплексі проводить низку заходів із захисту периметру ІС або об’єкту інформаційної діяльності (ОІД), де така ІС розташована, її систем управління (АСУ) та забезпечення доступу, мережевого обладнання та зовнішнього периметру ОІД, тощо.

Це передбачає проведення комплексу заходів, на кшталт [3]:

по-перше, визначення вимог до системи захисту (формування «політики безпеки»);

по-друге, здійснення вибору засобів захисту (формування «системи підтримки політики безпеки»);

по-третє, формування «механізмів захисту» (тобто, обрання способів, заходів і засобів захисту та впровадження їх в дію);

по-четверте, здійснення контролю цілісності та управління системою захисту (тобто, реалізація механізмів захисту).

Політика безпеки формується при цьому на підставі аналізу стану захищеності ОІД з системи ієрархічно підпорядкованих документів (моделей), що визначають (або встановлюють) порядок забезпечення безпеки інформації на ОІД, а також висувають вимоги з його підтримання. Класи, види та взаємозв'язок моделей, які використовуються для формування та аналізу політик безпеки подано на рис.3.3.

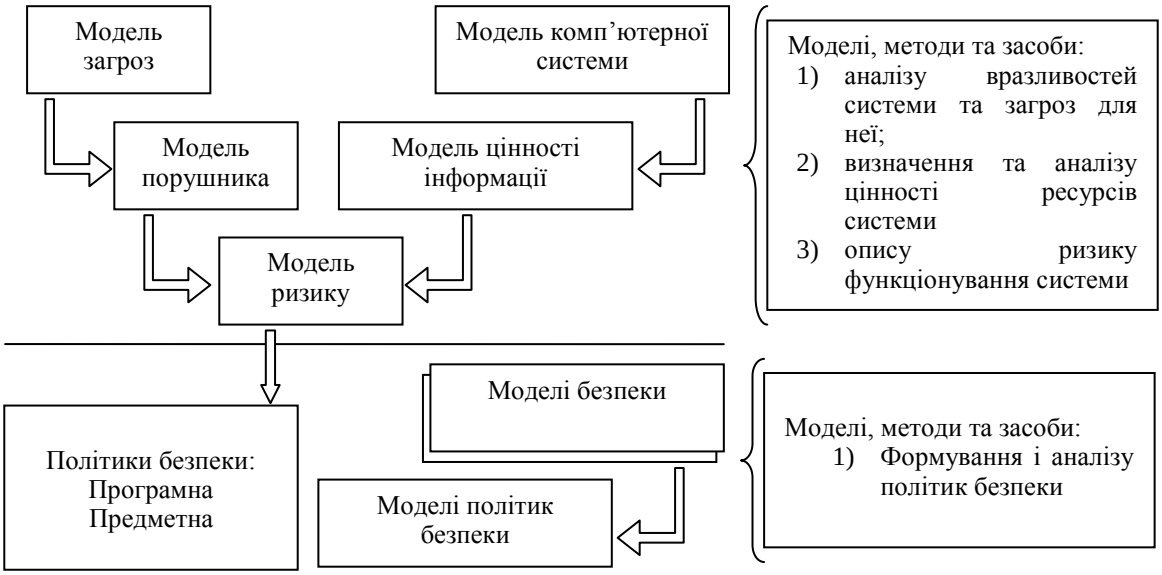


Рис.3.3 Класи, види та взаємозв'язок моделей,
які використовуються для формування та аналізу політик безпеки

Модель загроз формується при цьому з метою опису їх потенційно можливих джерел та визначення того збитку, що може бути завданий, наприклад, дією шкідливих програм, фальшивим ПЗ та злоякісними шифруючими кодами. Зважаючи на таке одним із проблемних питань стає визначення внеску зазначеного контенту на забезпечення виконання АСУ ОКІ завдань з накопичування, переробки та збереження інформації. Не менш важливим до того ж має бути завдання щодо визначення можливих методів протидії деструктивному впливу шкідливих програм, завідомо фальшивого ПЗ та злоякісних шифруючих кодів, а також оцінювання стану захищеності від стороннього кібернетичного впливу АСУ ОКІ в цілому.

3.1 Часткова модель загроз безпеці перспективних гарантоздатних АСУ ОКІ

Першою й найбільш неоднозначною серед низки моделей, які використовуються для формування та аналізу політик безпеки є модель загроз (рис.3.4) [4, 5].

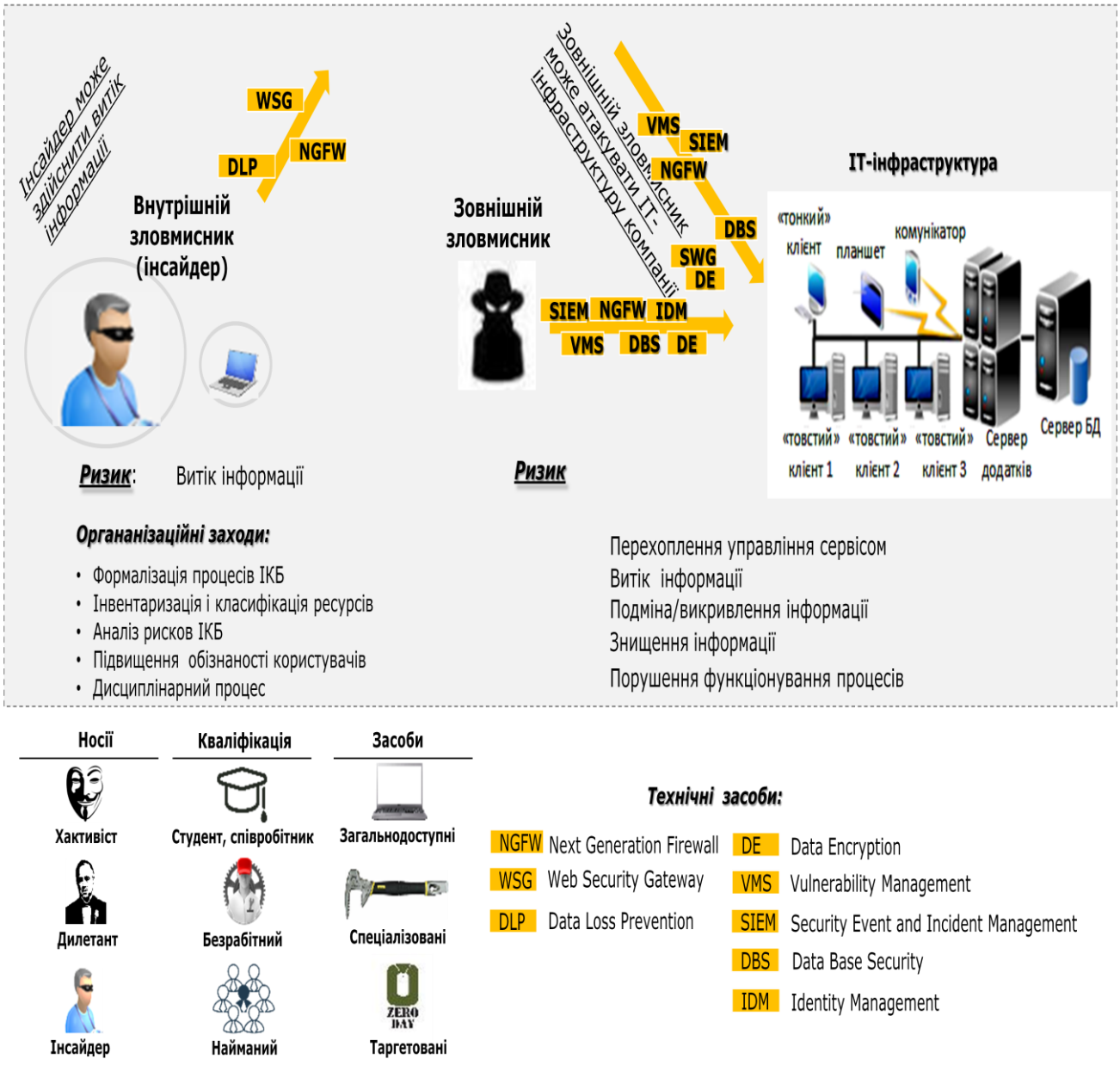


Рис.3.4 Модель загроз АСУ ОКІ

Загрози інформації в АСУ ОКІ можуть мати при цьому як суб'єктивну, так і об'єктивну природу. Джерелом загроз суб'єктивного характеру виступатимуть навмисні чи ненавмисні дії осіб (користувачів, персоналу, зловмисників тощо), які можуть отримати віддалений доступ до ресурсів АСУ з використанням каналу доступу до мережі Інтернет, або фізичний доступ в приміщення, де розміщена АСУ чи до її машинних носіїв інформації. Рейтинг загроз інформації, що обробляється з використанням потужностей АСУ ОКІ подано на рис.3.5 [6].

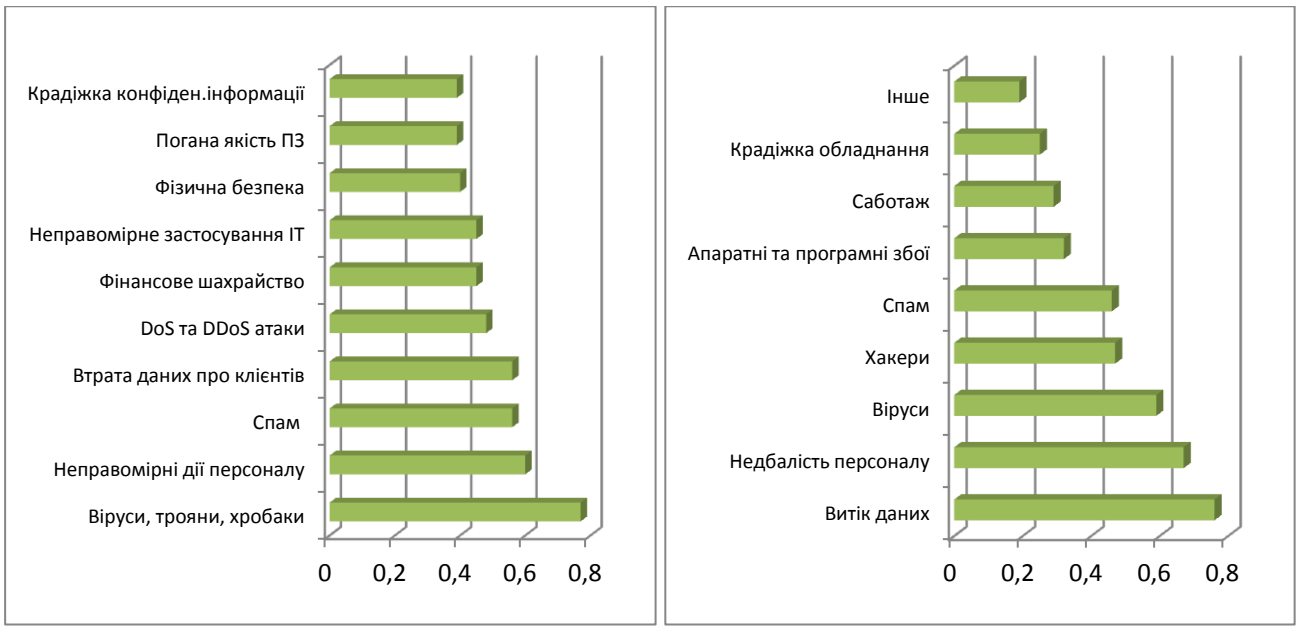


Рис.3.5 Рейтинг загроз АСУ ОКІ

Абстрактний формалізований опис типів загроз, джерел їх виникнення, методів і засобів здійснення загроз, а також очікуваних наслідків наведено в таблиці 3.1 (Формалізована модель загроз АСУ ОКІ (часткова)) та Додатку А (Формалізована модель загроз АСУ ОКІ (повна)).

3.2 Семантична модель протиборства системи захисту перспективної гарантоздатної АСУ ОКІ та атакуючої сторони

Інструментом реалізації загроз щодо АСУ ОКІ є атаки (кібератаки) – навмисні дії, що здійснюються за допомогою засобів електронних комунікацій та спрямовані:

- на порушення конфіденційності, цілісності, доступності електронних ІР, що обробляються (передаються, зберігаються) на ОКІ, отримання НСД до таких ресурсів;
- на порушення безпеки та сталого і надійного режиму функціонування АСУ;
- проти об’єктів захисту із застосуванням потужностей АСУ та засобів електронних комунікацій.

На підставі аналізу наукових публікацій щодо реалізації атак, зокрема кібератак з шифруванням інформації [7, 8], можливо визначити типову послідовність їх етапів (модель атак) в АСУ ОКІ (комп’ютерних системах – КС) за допомогою ПЗ реалізації атак (ПЗРА).

Модель включає вісім фаз активних дій порушника безпеки (рис. 3.6), а саме:

Таблиця 3.1

Формалізована модель загроз АСУ ОКІ (часткова)

Тип загрози	Джерело загрози	Можливий метод (спосіб) реалізації атаки	Наслідки		
			К	Ц	Д
Несанкціоноване внесення змін в комплекс технічного захисту, ПЗ та компоненти інформаційного забезпечення	Апаратура, Персонал, Користувачі	Недостатній контроль			
Загрози порушення технології введення / виведення видової інформації. Копіювання вихідних документів, магнітних та інших носіїв інформації	Персонал, користувачі	Неуважність, недбалість, некомпетентність	+	+	+
Загрози застосування портативної розвідувальної апаратури, що розміщується в транспортних засобах поруч з ОІД або безпосередньо на самому об'єкті	Апаратура, Персонал, Користувачі	Недотримання організаційних заходів	+		
Загрози використання оптичних засобів, дистанційне фотографування тощо для копіювання інформації	Апаратура, Персонал, Користувачі	Недотримання організаційних заходів	+		
Загрози читання видової/залишкової інформації («сміття»), що виводиться на екран, роздруковується або зберігається на запам'ятовуючих пристроях	Персонал, Користувачі	Знаходження в службових приміщеннях сторон.осіб	+		
Загрози розкрадання магнітних носіїв та документів, отримання не облікованих копій	Апаратура, Програми, Персонал, Користувачі	Отримання сторонніми особами доступу до мережевих накопичувачів інформації	+		
Збір за допомогою спеціальних засобів ЕМ випромінювань АСУ (пристроїв відображення інформації, процесорів, ліній зв'язку тощо)	Апаратура	Каналами побічних ЕМВ і наведень	+		
Збір за допомогою спеціальних засобів побічних наведень на доп.засоби та системи (мережі теплопостачання, системи вентиляції, шини заземлення, тощо)	Апаратура	Каналами побічних ЕМВ і наведень	+		
Незаконне підключення до апаратури АСУ, систем електроживлення та заземлення	Апаратура, Персонал, Користувачі	Каналами побічних ЕМВ і наведень	+	+	+
Використання закладних і дистанційних підслуховуючи пристроїв	Апаратура, Персонал, Користувачі	Каналами побічних ЕМВ і наведень	+		
Прослуховування телефонних розмов	Апаратура, Персонал, Користувачі	Каналами ПЕМВіН Несанкціоноване підключення	+		
Зміна умов фізичного середовища: аварії, стихійні лиха	Оточуюче середовище	Стихійні лиха, кліматичні зміни		+	+
Тимчасова відсутність персоналу (хвороба, відрядження, відпустка)	Персонал, користувачі	Сімейні обставини, епідемії, службова необхідність тощо		+	+
Порушення порядку зберігання та обліку документів, носіїв інформації, даних, ТЗ	Персонал, користувачі	Неуважність, недбалість, некомпетентність	+	+	+
Загрози застосування програмних вірусів (включення в ПЗ програмних закладок типу «бомби», «троянського коня» тощо)	Програми, Персонал, Користувачі	Використання неперевіреного ПЗ	+	+	+
Загрози застосування програмних закладок (недоліки у мовах програмування, операційних системах тощо)	Програми, Персонал, Користувачі	Використання неперевіреного ПЗ	+	+	+
Загрози впровадження і застосування забороненого політикою безпеки ПЗ (неліцензійного) або несанкціоноване використання ПЗ	Програми, Персонал, Користувачі	Використання неперевіреного ПЗ	+	+	+
Загрози здійснення заходів, що можуть призвести до розголошення паролю адміністратора АСУ або до його втрати, тощо	Персонал, користувачі	Неуважність, недбалість, некомпетентність		+	+
Загрози здійснення заходів, що можуть призвести до відмови АСУ, руйнування програмно-апаратних та інформаційних ресурсів	Персонал, користувачі	Неуважність, недбалість, некомпетентність		+	+
Загрози одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача ("маскарад").	Програми, Персонал, Користувачі	Отримання сторонніми особами доступу до ресурсів АСУ	+	+	+
Загрози «імітації дій користувача» та виконанні операцій прийому/передавання даних від його імені	Апаратура, Програми, Персонал, Користувачі	Підключення порушника до обчислювальної мережі та отримання відомостей про конфігурацію мережевих пристроїв, тип ПЗ	+		

НАСЛІДКИ: К – порушення конфіденційності; Ц – порушення цілісності; Д – порушення доступності

Рис.3.6. Модель атаки в АСУ ОКІ за допомогою ПЗ реалізації атак

фаза 1 – «***Розвідка***». Збирання інформації про обєкт атаки з метою виявлення діапазону адрес, тощо. Пошук відкритими джерелами за допомогою запитів Whois. Засоби: UseNet, пошукові сервери, будь-які клаєнтські програми UNIX для доступу до баз даних. Створення так званих «приманок»;

фаза 2 – «***Розробка***». Сканування об'єкта атаки з метою пошуку найбільш доступних способів проникнення в систему. Прийоми: Ping – прослуховування, сканування TCP/UDP портів, визначення версії ОС. Засоби: fPing, SuperScan, SiPhon. Розробка власних ПЗ реалізації атак (ПЗРА);

фаза 3 – «***Маскування***». Усунення ознак, які пов’язують ПЗРА та спосіб його застосування з реальним розробником, та/або створення фіктивних ознак, що ототожнюються з непричетними до кібератаки суб’єктами. Визначення тактики приховування реального маршруту (адрес проміжних вузлів глобальної мережі) спроб проникнення в КС;

фаза 4 – «***Проникнення***». Подолання системи захисту та проникнення ядра ПЗРА в програмне середовище КС. Отримання доступу до ресурсів. Прийоми: перехоплення паролів, захват спільних IP та /або паролів, переповнення буфера. Засоби: TCPDump, LOphtCrack тощо;

фаза 5 – «***Підготовка***». Отримання привілеїв з метою встановлення повного контролю над системою та збирання ПЗРА в автоматичному або автоматизованому режимах інформації з її окремих модулів. Прийоми: злам паролів. Засоби John, LOphtCrack, getAdmm.sechole;

фаза 6 – «***Реалізація***». Створення вільного доступу до системи та інших довірених систем, виявлення та ідентифікація підсистем (елементів) КС у її запам’ятовуючих пристроях. Використання виявлених зашифрованих, знищених або модифікованих ресурсів для розкриття конфіденційної інформації. Прийоми: виявлення довірених відношень, пошук незашифрованих паролів. Засоби: Rhosts, секрети LSA, файли конфігурації, системний реєстр [9];

фаза 7 – «***Витік***». За необхідності, створюється канал прихованої передачі зібраних даних з використанням методів стеганографії, процедури стискання даних з наступним шифруванням, фізичного переносу під час підключення зовнішніх пристроїв тощо. Наприклад, для створення прихованого каналу передавання даних можливо використовувати 32-х бітове поле *ISN* в *TCP* протоколі, яке призначене для

забезпечення взаємодії віддаленого клієнта з сервером. Слід зауважити, що досить невеликий обсяг трафіку може бути не виявлений стандартними методами його аналізу;

фаза 8 – «***Самоліквідація***». Приховування слідів атаки. Етап реалізується автоматично, в разі настання в КС певних обставин (наприклад, визначеного часу), або автоматизовано на підставі отримання команди ззовні.Прийоми: очистка журналів, системних логів. Засоби: Zap, графічний інтерфейс утиліти просмотра журналу подій.

Найбільш вживаними згідно статистики при цьому є DDoS-атаки. Їх суть полягає в такому: через керуючу консоль зловмисник зв'язується з головними серверами ботнету, з яких безпосередньо відправляються команди інфікованим хостам. Вони в свою чергу формують сотні запитів різних типів, якими атакується вузол-мішень.

Це стосується й атак, які використовують прорахунки проектування та формують сотні запитів різних типів, якими атакується вузол-мішень в реалізації криптографічних ПЗРА, що не були виявлені під час їх проектування [10, 11], а також шкідливих програм, завідомо фальшивого ПЗ та злоякісних шифруючих кодів (табл.3.2) , зокрема такого шкідливого криптографічного вірусу, як WannaCry [8, 12].

Таблиця 3.2

Співвідношення загроз і послуг безпеки на прикладі застосування шкідливих програм, завідомо фальшивого програмного забезпечення та злоякісних шифруючих кодів

Загроза	Послуга	Спосіб реалізації атаки	Застосування	Наслідки
Віруси	Ц,Д	Ransomware (програма, що блокує роботу ПЕОМ користувача)	Застосовується для вимагання коштів з користувачів за розблокування їх ПЕОМ	Локальне проникнення в комп'ютерну мережу
Сніфер	К,Ц,Д	Rootkit (набір программ, що встановлюється на ПЕОМ відразу після отримання хакером прав суперкористувача)	Застосовується для приховування слідів присутності зловмисника або шкідливої програми в системі	
Сканер	К,Ц,Д			
Кейлогер	К,Ц,Д			
Троянські програми	К,Ц,Д	Троянський кінь (програма, яка видає себе за безпечний та корисний за стосунок)	Застосовується як спливаюче вікно з інформацією, що переконує жертву встановити програму на її ПЕОМ	
Перехоплення	Д	SpyWare (моніторинговий ПЗ, несанкціоновано, без сповіщення користувача, встановлюється і вживається на ПЕОМ)	Застосовується для оцінювання та виявлення уразливостей ПЕОМ	
Диверсії	Ц,Д	КНОВЕ (програма, яка до перевірки антивірусом є абсолютно безпечною)	Застосовується лише після перевірки програми антивірусом та передбачає заміну коду програми на інший	Віддалене проникнення в комп'ютерну мережу
Крадіжка	К,Ц,Д	Шляхом застосування технологій віддаленого адміністрування	Застосовується для отримання несанкціонованого доступу	
Апаратні збої	К,Ц,Д	BrowserHijackers (програма, що при завантаженні змінює початкову сторінку або сторінку, яка запитується)	Застосовується для заміни початкової сторінки або сторінки, яка запитується на дані про помилки інших сторінок, які користувач не запитував	
Перекручування	К	Bot-коди (програми, що призначені для автоматизації контролю та проведення адміністрування)	Застосовується для контролю параметрів та адміністрування каналів IRC (Internet Relay Chat)	

З урахуванням викладеного уявляється можливим сформувати наступну семантичну модель протиборства захисту АСУ ОКІ та атакуючої сторони (табл.3.3).

Таблиця 3.3

Семантична модель протиборства захисту АСУ ОКІ та атакуючої сторони

Дія	Час початку	Етап	Методика дій захисту АСУ ОКІ
A_1	t_1	Вибір об'єкту атаки	Апріорна оцінка загрози
A_2	t_2	Пошук вразливості	Моніторинг портів та підключення пристроїв
A_3	t_3	Вбудовування Backdoor (лазівки), модифікація коду системи	Контроль несанкціонованих дій
A_4	t_4	Завантаження та запуск шкідливого коду	Контроль НСД, обчислення функції прийняття рішення
A_5	t_5	Активація асиметричного перетворення, виклик стандартних функцій PRNG, CryptoAPI тощо	Контроль, перехоплення звернень, підміна фіктивною функцією
A_6	t_6	Активація симетричного перетворення, виклик стандартних функцій PRNG, CryptoAPI тощо	Контроль, перехоплення звернень, підміна фіктивною функцією
A_7	t_7	Читання файлів за переліком форматів (розширень)	Контроль і управління доступом
A_8	t_8	Заміна розширення зашифрованого файлу на нестандартний формат	Контроль та блокування процесу
A_9	t_9	Знищення ключових даних шляхом звернення к відповідним функціям	Контроль та блокування процесу
A_{10}	t_{10}	Відправлення зашифрованих даних зловмиснику	Контроль та блокування процесу
A_{11}	t_{11}	Перезавантаження системи	Контроль та блокування процесу
		Закінчення атаки	Пошук ключів у ОЗП, RAM

Для семантичної моделі часові інтервали мають наступні обмеження:

$$\begin{cases} t_{11} - t_1 \le T_{атаки,max} \\ t_{i+1} - t_i \le \Delta_i \end{cases}, \tag{3.4}$$

де $T_{атаки,max}$ – загальна тривалість атаки, Δ_i – середній час між етапами атаки.

В умовах (3.4) на кожному етапі $\{A_i, i = \overline{1,11}\}$ ми розраховуємо функції прийняття рішення про атаку:

$$\vartheta_i(A_1, \quad \dots, \quad A_i) = \begin{cases} 1, якщо\ приймається\ рішення\ про\ атаку \\ 0, \quad в\ іншому\ випадку \end{cases}$$

Результати проведених комп'ютерних експериментів свідчать, про достатню ефективність запропонованого методу та можливість його широкого застосування в системах антивірусного захисту.

3.3 Процедура детектування та відновлення даних в перспективній гарантоздатній АСУ ОКІ

Відомо, що АСУ ОКІ створюються з метою задоволення потреб користувачів у забезпеченні надійного і своєчасного подання повної та достовірної інформації, а також її накопичуванні, переробці та збереженні. Ступінь виконання цих потреб повинна оцінюватися при цьому в умовах потенційно можливого впливу загроз,

зокрема шкідливих програм, завідомо фальшивого ПЗ та злоякісних шифруючих кодів, що впливатимуть передусім на порушення конфіденційності інформації та її цілісності, працездатності самої АСУ та/або доступності до інформації, що в ній циркулює тощо. Саме тому задача формування системи протидії такому впливу та відновлення зашифрованих даних, незважаючи на появу більш ефективних механізмів його виявлення, аналізу та оновлення баз його описів і правил виявлення – й нині є доволі гострою.

Важливим аспектом вирішення цієї задачі є пошук евристичних методів детектування, що мають більшу точність виявлення та реалізуються або шляхом періодичного контролю цілісності обчислювального середовища гарантоздатних АСУ ОКІ, або завдяки застосуванню дворівневої системи ідентифікації впливів таких програм, ідентифікації факту впливу та ідентифікації слідів впливу. Найбільш ефективною при цьому є система ідентифікації. В її основі знаходяться такі способи та методи детектування за допомогою професійних пакетів антивірусних засобів, як: сканування; евристичне сканування;CRC-сканування; антивірусний моніторинг та імунізація (табл.3.4) [13].

Таблиця 3.4

Механізми детектування шкідливих програм,
завідомо фальшивого програмного забезпечення та злоякісних шифруючих кодів

Найменування антивірусного засобу	Механізм				
	Сканування	Евристичне сканування	CRC сканування	Моніторинг	Імунізація
ADINF («Діалог-Наука»)			+		
DrWeb («Діалог-Наука»)		+		+	
AVP («Лабораторія Касперського»)	+			+	
Norton AntiVirus (Norton Inc.)	+			+	
McAfee SCAN	+				
Service Pack					+

Аналіз типових ситуацій впливу шкідливих програм, завідомо фальшивого ПЗ та злоякісних шифруючих кодів на інформаційні процеси в захищених ІС дозволив встановити, що їх дії, як специфічного виду комп'ютерних вірусів формально можна представити наступною послідовністю кроків [13]:

Крок 1. Перехоплення управління шляхом передачі помилкового запиту базового модулю ОС функцій на обслуговування переривань по виконанню програм;

Крок 2. Відновлення початкового вигляду програми, в яку впроваджено шкідливі програми, завідомо фальшиве ПЗ та злоякісні шифруючі коди;

Крок 3. Інфікування оперативної пам'яті комп'ютера;

Крок 4. Виконання шкідливих функцій з протиправного маніпулювання інформацією;

Крок 5. Повернення управління основній програмі.

Сутність відповідних цим крокам способів ідентифікації полягає в такому:

порівняння послідовності виконуваних контрольних точок у програмі з еталонною;

аналіз початку файлу на наявність кодів команди переходу або коду, який не відповідає реальній адресі її запуску та відноситься до типу контрольних операцій перевірки відповідності даних області значень;

аналіз векторів переривань, відповідних функцій завантаження і виконання програм, які також відносяться до типу контрольних операцій перевірки відповідності даних області значень.

Так як при виконанні даних кроків шкідлива програма (завідомо фальшиве ПЗ, злоякісні шифруючі коди) реалізує системні функції, операції виявлення повинні проводитися тільки компонентами ОС під управлінням її базового модуля. При цьому еталонна послідовність контрольних точок також повинна бути надійно захищеною.

Для відновлення зашифрованих даних, тобто вирішення задачі криптоаналізу, останнім часом все частіше застосовують так звану технологію «грубої сили», яка ґрунтується на можливості використання ресурсів різного роду аутсорсінгових центрів та застосовується для пошуку істинних значень застосованих ключів. Нескладно показати, що якщо кількість різних криптографічних ключів у симетричній криптосистемі дорівнює N, а максимальний час для відновлення інформації не повинен перевищувати T, тоді потужність обчислювача має бути що найменш $V \geq N/2T$ перевірених ключів в одиницю часу. Основні методи, що використовуються для цього можливо умовно розділити на декілька класів, а саме:

імовірнісно-статистичні методи (ІСМ) дослідження великих обсягів (до $N \approx 2^{100}$) вихідних послідовностей псевдовипадкових генераторів ключових даних або послідовностей, які зашифровані за допомогою засобів КЗІ;

методи ортогональних перетворень (МОП) вихідних аналогових та цифрових даних за методами Фур'є, Уолша, Уолша-Адамара, вейвлет - перетворень, обчислення функцій згортки та кореляції;

алгебраїчні та комбінаторні методи розв'язку (АКМР) систем лінійних або нелінійних рівнянь великої розмірності ($N \approx 2^{80} \div 2^{256}$) з викривленими правими частинами, розкладання великих чисел на прості множники ($N \approx 2^{1024} \div 2^{2048}$), знаходження дискретного логарифма в полі великого порядку ($N \approx 2^{1024} \div 2^{2048}$), знаходження кратності точки на еліптичної кривої тощо;

методи лінійного і динамічного програмування (МЛДП) розв'язку задач пошуку екстремумів функцій, заданих на просторі ключів (розкриття ключів типу підстановка або перестановка);

методи оптимізованого або повного перебору (МОПП) параметрів криптосистем;

змішані методи.

Серед ІСМ методів особливим значенням для криптоаналізу та найбільшою обчислювальною складністю характеризуються методи пошуку пар послідовностей за критерієм “нульових вертикальних біграм” (НВБ), методи пошуку суцільних та переривчастих повторів (ПСПП) за відповідним критерієм, а також різного роду комбінації цих методів. За їх допомогою можливо виявити випадки однаково зашифрованих повідомлень.

Складність зазначених методів можна оцінити такими величинами:

$$W_{НВБ} \approx K_1 \cdot C_N^2 \cdot 2 \cdot (M - m), \tag{3.5}$$

$$W_{ПСПП} \approx K_2 \cdot \left[\frac{M \cdot N}{L}\right] \cdot \lg\left[\frac{M \cdot N}{L}\right], \tag{3.6}$$

де N – кількість послідовностей, що аналізуються; M – середня довжина послідовності; L – довжина повторення; m – мінімальна довжина “перетинання” двох послідовностей для отриманні сталого статистичного виводу (нормальної роботи критерію); K_1, K_2 - постійні коефіцієнти, що залежать від системи команд процесору та використаної мови програмування.

З формул (3.5) та (3.6) можливо отримати практичні оцінки для складності розв’язку відповідних задач. Наприклад, якщо кількість послідовностей, що аналізуються дорівнює $N = 10^5$, їх середня довжина становить $M = 10^3$ біт, а мінімальна довжина “перетинання” - $m = 10^2$, то складність розв’язку задачі підбору пар за критерієм НВБ оцінюється величиною $W_{НВБ} \approx 9 \cdot 10^{12}$. Це означає, що за наявності обчислювальної потужності системи w понад 10^8 елементарних операцій в секунду, задача комплектування може бути вирішена протягом доби. Якщо ж у попередніх умовах довжина повторення L дорівнюватиме 10, то нескладно бачити, що за наявності обчислювальної потужності $w \geq 7 \cdot 10^7$ операцій за секунду повтори довжиною в 10 біт можливо виявити за одну добу. Наведені оцінки мають значення для викладення змісту третьої частини роботи та побудови атак на стійкі криптографічні системи із застосуванням технологій активного впливу у кібернетичному просторі на криптографічні примітиви, зокрема, генератори випадкових даних.

Зауважимо, що пошук повторів можливо здійснити значно швидше, якщо обчислювальна система має швидкісну пам’ять з прямим доступом відповідного об’єму. Наприклад, в умовах наведеного прикладу для фіксації усіх повторів довжиною 10 біт необхідно мати 2^{10} комірок пам’яті, у яких фіксують координати (номер послідовності, номер місця з якого починається повтор) кожного можливого повтору. При цьому розмір комірки безпосередньо залежить від об’єму вихідного

масиву та від ступеню нерівномірності розподілу зустрічаємості елементів послідовностей (в одному крайньому разі комірка може не містити жодного елемента, в другому – усі можливі координати десятиграм).

Використання МОП характерно для багатьох задач радіотехніки, тому побудова відповідних спеціалізованих обчислювальних систем в інтересах криптоаналізу полегшується за рахунок застосування різного роду готових апаратно-програмних прискорювачів. Проблеми їх застосування мають чисто технічний характер, обумовлений сумісністю різних платформ і форматів подання даних. Зокрема, під час дешифрування сигналів захищеної аналогової телефонії використовується швидке перетворення Фур'є для побудови різного роду цифрових фільтрів. Відомо, що фільтрація сигналів складними не рекурсивними фільтрами, які містять п'ятдесят і більш членів у математичних виразах, що їх описують та велике число повторних обчислень [14]. Якщо вхідний сигнал має M відліків, а нерекурсивний фільтр має N відгалужень (де $M > N$), для оцінки частотної характеристики фільтра потрібно $N \cdot M$ множень. Т.Стокхем [14] запропонував метод зменшення числа множень, що необхідні для оцінювання частотної характеристики фільтра. Він показав, що у випадку N у формі 2^n при правильно організованих обчисленнях число множень приблизно оцінюється такою величиною:

$$W \approx M \cdot \log_2 N . \qquad (3.7)$$

АКМР відіграли суттєву роль у розробці методів дешифрування потокових криптосистем покоління 60-80 років минулого сторіччя, але питання їх використання для цілей дешифрування сучасних криптосистем блокового типу залишається відкритим. Складність розв'язку систем лінійних рівнянь над двійковим полем F_2 класичним методом Гауса становить $W = n^3/3$, де n - число змінних [15]. У випадку системи лінійних рівнянь над полем із q елементів F_q складність розв'язку за методом І.В. Коновальцева оцінюється величиною: $W \approx K \cdot \dfrac{n^3}{\log_q N}$. (3.8)

Застосування АКМР дає можливість обмежити вимоги до потужності обчислювальної системи, але їх застосування можливе лише за умов знаходження ефективних способів лінеаризації функцій перетворень для конкретних сучасних алгоритмів. МЛДП досліджені достатньо глибоко. Їх найбільше застосування припало на 50-80 роки минулого сторіччя. На жаль, для сучасних криптосистем їх застосування, в силу ряду причин, залишається проблематичним. Застосування МОПП параметрів криптосистем, не зважаючи на досить велику довжину ключів сучасних криптосистем залишається одним з перспективних напрямів

дешифрування, оскільки у цьому випадку, вочевидь, просто вирішується подання ключового простору у вигляді об’єднання множин меншої потужності. Можливість розв’язання задач дешифрування при цьому визначається технологією побудови та архітектурою швидкодіючої спеціалізованої обчислювальної системи.

Для підвищення ефективності перелічених вище методів та уникнення суб’єктивізму, у задачах криптоаналізу все частіше застосовують, поряд з іншими, технології кластеризації [39]. Кластер – це система, що складається з потужного комп’ютеру, комунікаційного обладнання, ОС та мережних застосувань (рис.3.7).

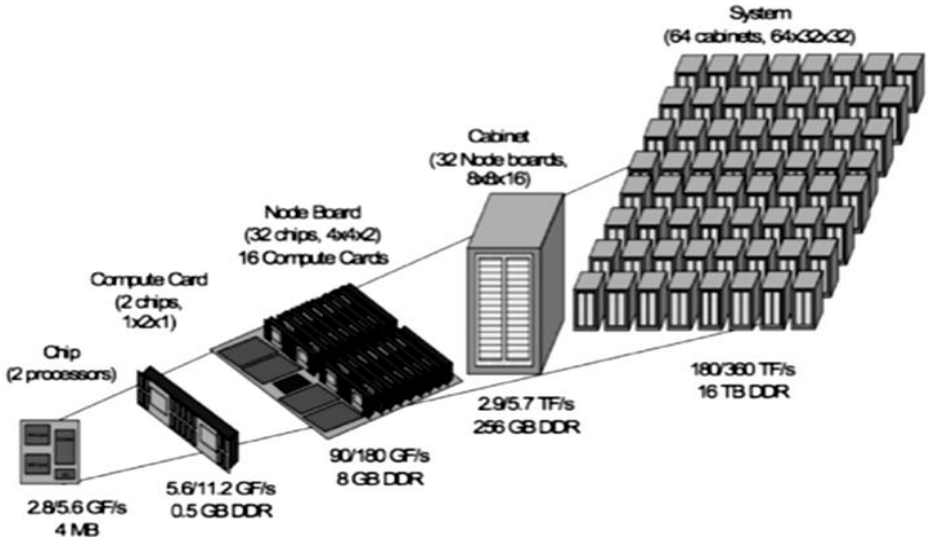


Рис. 3.7. Приклад “паралельної” ієрархії

Розпаралелювання операцій суттєво залежить при цьому від архітектури конкретної розподіленої обчислювальної системи. Найпростіші з них можна побудувати на базі локальних КМ, а спеціалізовані доцільно створювати на основі симетричних мультіпроцесорів (*SMP – Symmetric Multi-Processors*), які, в свою чергу, складаються з декількох однорідних процесорів і масиву спільної пам’яті.

Багатопроцесорні системи, що об’єднані у кластер, можуть бути охарактеризовані при цьому таким чином. Вони мають:

можливість одночасно та незалежно один від другого виконувати декілька програмних гілок;

розділяєму (спільну) або розподілену (індивідуальну) пам’ять, що забезпечується вибором відповідної адресної системи;

масштабовану архітектуру, тобто не встановлюють жорстких обмежень щодо апаратної платформи обчислювальних модулів, щодо обладнання і топології КМ, щодо конфігурації та діапазону потужності обчислювальних засобів.

Вузловим моментом при цьому вважається вибір метрики (міри близькості об’єктів), від якої залежить остаточний варіант розбивки задачі, наприклад,

відновлення зашифрованих даних, тобто вирішення задачі криптоаналізу, на групи/підзадачі за заданим алгоритмом. Враховуючи таке вибір домінуючої задачі з визначеної вибірки з R (розмір генеральної сукупності) можливих задач пропонується здійснювати за рахунок поєднання можливостей методів, що перелічені вище, з методами кластерного аналізу шляхом виділення в досліджуваній сукупності задач таких однорідних підмножин, щоб:

задачі усередині груп були, у прямому смислі, подібні (схожі) один з одним;

задачі з різних груп були б або взагалі не подібні, або ж суттєво відрізнялися.

Отриманий результат в даному випадку може суттєво залежати від наступних факторів: відсутності однозначно найкращого критерію якості кластеризації; невизначеності щодо попередньої кількості кластерів відносно деякого суб'єктивного критерію; залежності результату кластеризації від метрики (або міри близькості задач щодо відновлення зашифрованих даних), вибір якої також суб'єктивний і визначається експертом [16, 17].

Алгоритм реалізації методу, який пропонується для рішення поставленої задачі полягає в послідовному виконанні наступних кроків (рис.3.8).

Крок 1. Формування матриці (табл.3.5), елементами якої можуть бути:

– альтернатив-критеріїв C_{ik}^r, якщо використовується якісна шкала, де $k = \overline{1,Q}$ – кількість критеріїв/ознак, $i = \overline{1,N}$ - кількість альтернатив/підзадач;

– вихідної вибірки даних C_{ik}^r для r-ї задачі відновлення зашифрованих даних ($r = \overline{1,R}$) та p_k ознак по кожній з них, якщо використовується кількісна шкала.

Таблиця 3.5

Вхідна вибірка даних

Ознаки **Підзадачі**	p_1	---	p_k	---	p_Q
r_1	C_{11}	---	C_{1k}	---	C_{1Q}
---	---	---	---	---	---
r_i	C_{i1}	---	C_{ik}	---	C_{iQ}
---	---	---	---	---	---
r_N	C_{N1}	---	C_{Nk}	---	C_{NQ}

Крок 2. Приведення матриці C_{ik} до нормального виду за правилами:

а) для критерію ефективності (чим більше, тим краще):

$$C_{ik}^r = \frac{C_{ik} - C_k^{\min}}{C_k^{\max} - C_k^{\min}}; \tag{3.9}$$

б) для критерію (ознаки) вартості (чим менше, тим краще):

$$C_{ik}^r = \frac{C_k^{\max} - C_{ik}}{C_k^{\max} - C_k^{\min}}; \tag{3.10}$$

де $C_k^{\max}$ та $C_k^{\min}$ – максимальне та мінімальне значення k-го критерію (ознаки) на всьому наборі альтернатив/підзадач;

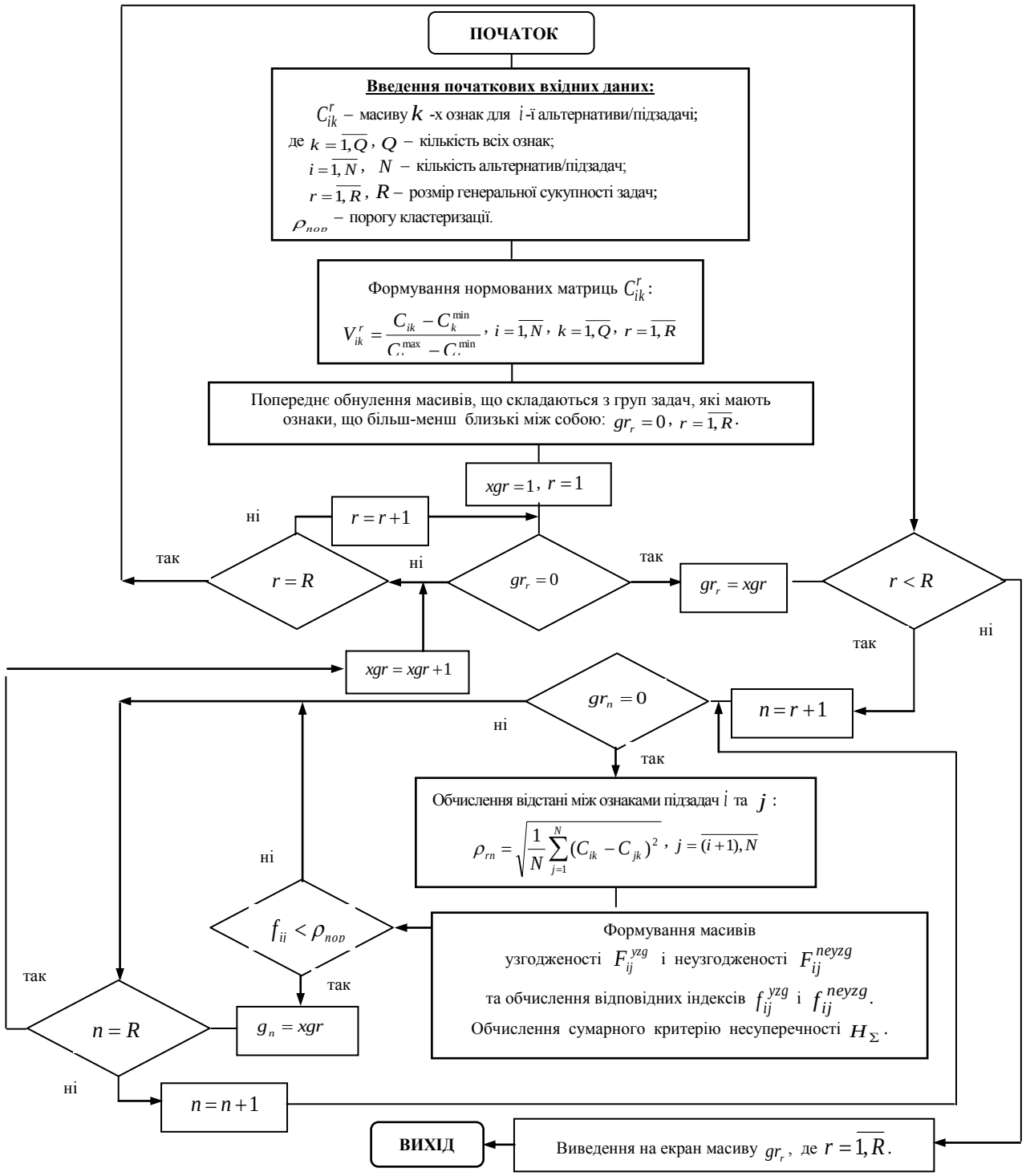


Рис.3.8. Алгоритм порівняльного оцінювання підзадач відновлення зашифрованих даних із застосуванням методів кластеризації

Крок 3. Формування матриці близькості $M^{blizk}(r_i,r_j)$, елементи якої (ρ_{ij}) будуть визначатися як між точкові відстані між пари альтернатив r_i та r_j:

$$\rho_{ij}=\sqrt{\frac{1}{Q}\sum_{k=1}^{Q}(C_{ik}-C_{jk})^2},\ j=\overline{(i+1),N}. \qquad (3.11)$$

Крок 4. За матрицею близькості для пари альтернатив/підзадач r_i та r_j:

1) поділ множини з R задач на підвибірки (диполі) близько розташованих підзадач $A \cap B$. Множина узгодженості має включати при цьому всі критерії (ознаки) з матриці близькості $M^{blizk}(r_i, r_j)$, за якими альтернатива r_i буде переважати альтернативу r_j: $F_{ij}^{yzg} = \{k | \rho_{ik} > \rho_{jk}\}$ і навпаки множина неузгодженості включатиме всі інші критерії (ознаки) – $F_{ij}^{neyzg} = \{k | \rho_{ik} < \rho_{jk}\}$;

2) довизначення (регуляризація) сформованих кластеризацій A і B шляхом додаткової перевірки та поділу множини підзадач на підмножини $C \cap D$ за правилом:

для диполів, що мають непарні номери, об'єкти, які належать A, відносяться до C;

для диполів, що мають непарні номери, об'єкти, які належать B, відносяться до D;

для парних номерів диполів – навпаки.

3) обчислення за формулою 3.11 міжточкових відстаней для підвибірок $A \cap B$ і $C \cap D$.

Пункти а), б) та в) повторюватимуться до тих пір, поки всі підзадачі не увійдуть до множин $A \cap B$ та $C \cap D$, або якщо мінімальна відстань між сформованими групами перевищить деяке критичне значення. Тоді головною умовою є виконання вимоги: протилежні вершини (підзадачі) мають відноситися до різних множин.

Крок 5. Здійснення перебору гіпотез про число кластерів H_{AB} для підвибірок $A \cap B$ і H_{CD} для підвибірок $C \cap D$ та обчислюються індекси, що відповідають масивам узгодженості і неузгодженості:

$$H_{AB} = \frac{h - \Delta h}{h} \to \min, \quad H_{CD} = \frac{h - \Delta h}{h} \to \min, \tag{3.12}$$

де h – кількість усіх кластерів, виділена на вибірках $A \cap B$ та $C \cap D$;

Δh – кількість кластерів, що подібні один до одного;

Крок 6. Проведення перебору кластеризацій за сумарним критерієм несуперечності H_{Σ}, та визначення порогів домінування шляхом порівняння індексів узгодженості – f_{ij}^{yzg} і неузгодженості – f_{ij}^{neyzg} з порогом кластеризації – $\rho_{їîð}$:

$$H_{\Sigma} = \frac{1}{2}(H_{AB} + H_{CD}) \to \min. \tag{3.13}$$

Оптимальній кластеризації [18] відповідатиме випадок, коли $H_{\Sigma} \to 0$.

Значення порога кластеризації – $\rho_{їîð}$ задається особою, що уповноважена приймати рішення.

Порівняння підзадач з оптимальної кластеризації здійснюється за правилом:

$$\text{якщо } f_{ij}^{yzg} > \rho_{ïîð} \text{ або } f_{ij}^{neyzg} < \rho_{ïîð}, \text{ то } r_i > r_j. \quad (3.14)$$

Реалізація запропонованого алгоритму дасть змогу за сумарним критерієм несуперечності або індексами домінування прийняти рішення щодо раціонального розподілу множини з R задач на групи та сформувати деревоподібну ієрархічну структуру з N підзадач в кожній.

3.4. Модель оцінки стану захищеності перспективної гарантоздатної АСУ ОКІ від загроз порушення цілісності, конфіденційності та доступності

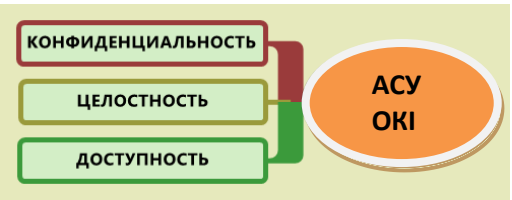
Завдання щодо оцінки стану захищеності обраного варіанту побудови перспективної гарантоздатної АСУ ОКІ від загроз порушення цілісності, конфіденційності та доступності вирішується з метою оцінки подій, які шляхом потенційно можливого впливу на АСУ прямо або опосередковано можуть завдати збитку її власникам і користувачам. Такі події класифікуються за такими основними ознаками, як: мета реалізації, джерела, засоби, методи і наслідки, принципи, характер та способи впливу на певний об’єкт (розділ 1.1.1 даної роботи). Захист від їх деструктивного впливу зосереджується, як правило, на рішення двох основних груп задач [19 – 27]:

по-перше, заборона порушнику НСД до інформації у зловмисних цілях;

по-друге, своєчасне і повне задоволення інформаційних потреб користувачів.

Зазначені задачі реалізуються в процесі технічного та/або криптографічного захисту інформації. Технічний захист в свою чергу передбачає захист інформації від витоку технічними каналами та захист АСУ і оброблюваної в ній інформації від НСД, а криптографічний – реалізацію таких методів криптографічного перетворення, як кодування та/або шифрування інформації.

Відомо, що з позицій класифікації кібернетичних злочинів і загроз за схемою, пропонованою Конвенцією Ради Європи 2001 року по боротьбі з кіберзлочинністю з урахуванням моделі CIA «Confidentiality-Integrity-Availability», а також стандартів ISO 27001 та ISO 27002 найбільшу небезпеку АСУ та ОКІ в цілому становлять загрози за метою реалізації. Вони, як відомо, полягають у порушенні конфіденційності інформації та її цілісності, працездатності та/або доступності до АСУ та інформації, що в ній циркулює (рис.3.9) [28, 29].



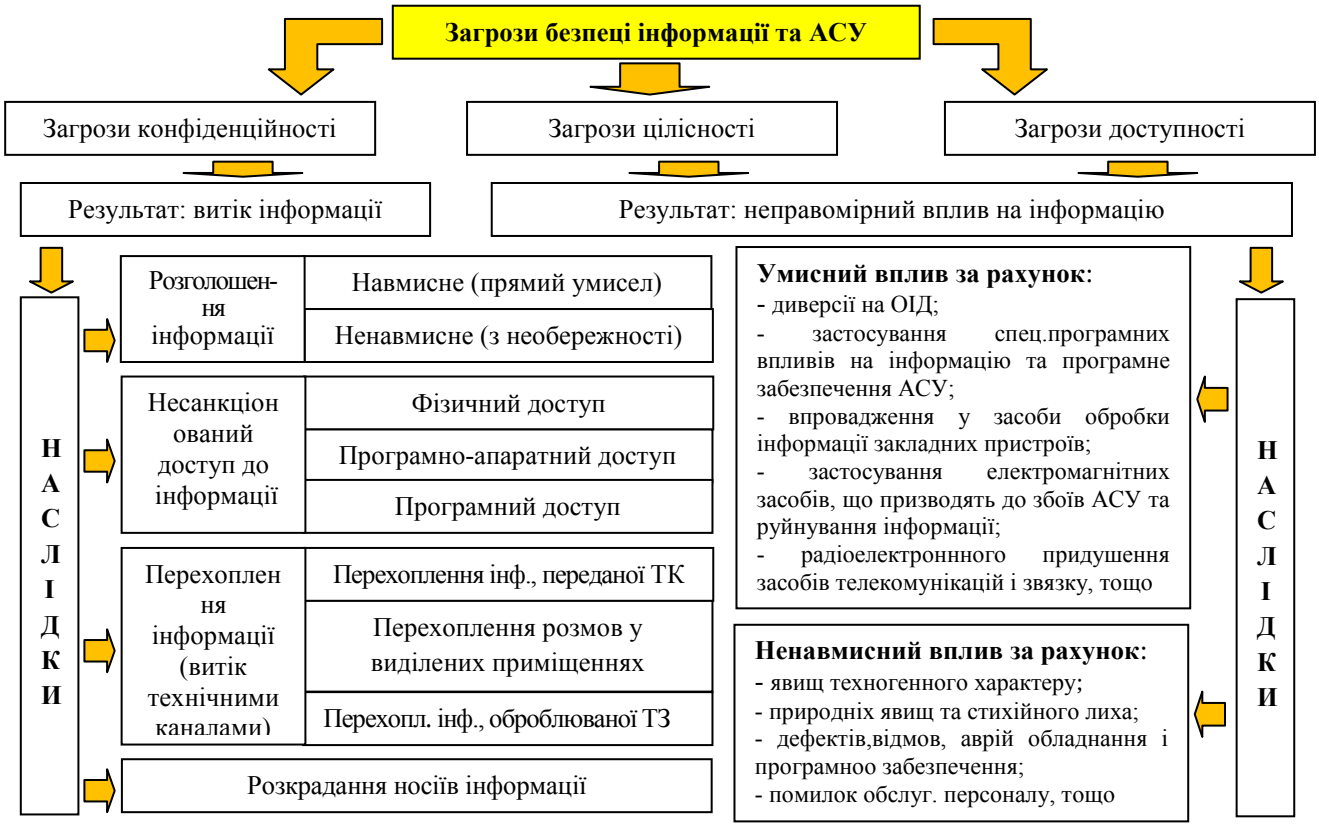


Рис.3.9. Головні ознаки порушення цілісності і конфіденційності інформації та доступності до неї

При цьому *до загроз порушення конфіденційності інформації в АСУ* згідно з [30 - 34] належать, як правило, спроби несанкціонованого: читання або копіювання як відкритої, так і конфіденційної інформації, імпорту або експорту такої інформації, а також обміну нею між елементами обчислювальної мережі, що відносяться до різних класів захищеності тощо. Вони ймовірно можуть бути реалізовані порушником за умови подолання ним [35]:

організаційних заходів обмеження доступу до ОІД та приміщень ($p_{озод}$);

фізичних заходів обмеження доступу до ОІД та приміщень ($p_{фзод}$);

апаратних засобів захисту каналів витоку інформації на ОІД ($p_{аззкв}$);

апаратних засобів управління доступом *(брандмауерів)* до ресурсів АСУ ($p_{азуд}$);

ПЗ адміністрування доступу на ресурсів АСУ ($p_{пзад}$);

ПЗ ідентифікації та автентифікації користувачів ($p_{пзіак}$);

ПЗ захисту від вірусних атак ($p_{пззва}$).

Виходячи з того, що подолання програмно-апаратних засобів управління доступом ($p_{пазуд} = p_{азуд} \cdot p_{пзад}$) є ймовірністю події, яка складається з $p_{азуд}$ та $p_{пзад}$, а також враховуючи підхід, викладений у [36, 37] ймовірність отримання порушником

НСД до ресурсів АСУ та/або інформації за рахунок подолання засобів управління доступом ($p_{нсд}$) може бути визначена з виразу

$$p_{нсд} = p_{пазуд} \cdot \left[1 - (1 - p_{озод}) \cdot (1 - p_{фзод}) \cdot (1 - p_{пзіак})\right]. \quad (3.15)$$

Подальше розкриття змісту інформації з обмеженим доступом може статися, як відомо з [38], лише за умови якщо порушник після її отримання:

знає мову, якою інформація подається (ймовірність події - $p_{мова}$);

знає і може застосовувати ПЗ або апаратуру криптоперетворення ($p_{пзктп}$);

має ключі або ключові набори для криптоперетворення ($p_{ключі}$).

Виходячи з такого ймовірність подолання системи криптографічного захисту ($p_{кзі}$) з урахуванням положень [38] може бути визначена з виразу:

$$p_{кзі} = p_{мова} \cdot p_{пзктп} \cdot p_{ключі}. \quad (3.16)$$

З урахуванням такого ймовірність отримання порушником НСД до ресурсів АСУ та/або інформації, яка в АСУ обробляється може бути визначена таким чином:

$$p_{нсд}^{кзі} = p_{нсд} \cdot p_{кзі} \quad (3.17)$$

Враховуючи, що інформація в АСУ може бути втраченою й під час її обробки через витік технічними каналами (ймовірність події - $p_{аззкв}$) або завдяки низці вдалих кібернетичних атак (ймовірність події - $p_{пззва}$) загальна ймовірність порушення конфіденційності інформації в АСУ з подоланням зазначених засобів захисту матиме вид:

$$p_{поруш}^{конфід.} = 1 - \left(1 - p_{нсд}^{кзі}\right) \cdot (1 - p_{аззкв}) \cdot (1 - p_{пззва}) \quad (3.18)$$

До загроз порушення цілісності інформації в АСУ, як відомо [30 – 34], належать: несанкціонована модифікація та/або видалення програм і даних; вставка, зміна або видалення даних в елементах протоколу в процесі обміну між абонентами обчислювальної мережі; втрата даних у результаті збоїв, порушення працездатності елементів обчислювальної мережі або некомпетентних дій суб'єктів доступу тощо. Ймовірно, з урахуванням положень [38], вони можуть бути реалізовані порушником за умови подолання:

по-перше, організаційних і фізичних заходів обмеження доступу до ОІД та приміщень ($p_{озод}$, $p_{фзод}$), програмно-апаратних засобів управління доступом ($p_{пазуд} = p_{азуд} \cdot p_{пзад}$) та програмних засобів ідентифікації та автентифікації користувачів ($p_{пзіак}$), які, як і при аналізі загроз конфіденційності інформації, визначаються ймовірністю $p_{нсд}$;

по-друге, засобів захисту цілісності від загроз мережевої інфраструктури ($p_{зцзмі}$);

по-третє, засобів захисту цілісності інформації від спеціальних впливів

технічними каналами ($p_{зцсвтк}$);

по-четверте, засобів контролю та поновлення цілісності інформації ($p_{кпці}$).

По аналогії з алгоритмом аналізу та протидії загрозам порушення конфіденційності інформації в АСУ ймовірність порушення неавторизованим користувачем цілісності інформації може бути визначена з виразу

$$p_{поруш}^{цілісн} = p_{кпці}\left[1-\left(1-p_{нсд}\right)\cdot\left(1-p_{зцсвтк}\right)\cdot\left(1-p_{зцзмі}\right)\right] \qquad (3.19)$$

До загроз порушення доступності інформації в АСУ згідно з [30 – 34] відноситься: повторення або вповільнення елементів протоколу; придушення обміну в мережі; використання помилок або недокументованих можливостей служб і протоколів передачі даних для ініціювання відмови в обслуговуванні; перевитрата обчислювальних або мережевих ресурсів тощо. Вони, як і в попередніх випадках, можуть бути реалізовані за умови подолання порушником систем управління доступом до ІР в АСУ (ідентифікації, автентифікації, надання певних повноважень чи привілеїв, з наступною їх перевіркою під час кожної із спроб доступу до ресурсів) та фільтрації.

При цьому стійкість системи управління доступом (в розумінні ймовірності її не подолання) визначається стійкістю процесів ідентифікації та автентифікації самого адміністратора безпеки, як користувача з найширшими повноваженнями:

$$p_{ссуд} = 1 - p_{нсд}. \qquad (3.20)$$

Ця задача може вирішуватися застосуванням в АСУ засобів фільтрації типу міжмережних екранів (*firewall*, брандмауерів), сервісів-посередників (*proxyservices*) тощо. При середній тривалості обслуговування в АСУ одного запиту і пуассонівському законі розподілу ймовірностей впливу, ймовірність того, що під час звернення до ресурсу він уже використовується, згідно [36, 37] дорівнює:

$$p_{рес.}^{викор} = 1 - p_0 = 1 - \exp\left\{-t_{рес.}^{викор}\cdot\lambda_{зап}\right\}, \qquad (3.21)$$

де p_0 – ймовірність відсутності впливів (ймовірність того, що на певному часовому інтервалі виникне рівно нуль впливів); $t_{рес.}^{викор} = (T_{кі} - \Delta T_{кі})/n_{io}$ – середнє значення часу використання ресурсу; $T_{кі}, \Delta T_{кі}$ –періодичність і тривалість контролю цілісності; n_{io} – кількість інформаційних об’єктів, що потребують використання на інтервалі часу $(T_{кі} - \Delta T_{кі})$; $\lambda_{зап}$ – загальна інтенсивність впливів ($1/\lambda_{зап} \le t_{рес.}^{викор}$ - умова переходу захищеного ресурсу до режиму штучної відмови).

Враховуючи таке ймовірність порушення доступності ресурсу з урахуванням положень [38] дорівнюватиме:

$$p_{поруш}^{доступ} = 1 - \left(1 - p_{рес.}^{викор}\right)\cdot\left(1 - p_{ссуд}\right). \qquad (3.22)$$

Виходячи з наведених вище формульних залежностей стан захищеності обраного варіанту побудови перспективної гарантоздатної АСУ ОКІ від стороннього кібернетичного впливу та загроз, що класифікаються за метою реалізації може бути, як результат, знайдений з наступного виразу:

$$P_{стан.захищ}^{K_q^{total}} = 1 - \left(1 - P_{поруш}^{конфіден}\right) \cdot \left(1 - P_{поруш}^{цілісн}\right) \cdot \left(1 - P_{поруш}^{доступ}\right). \qquad (3.23)$$

На підставі отриманих результатів особа, що приймає рішення зможе сформувати рекомендації з вибору методів, заходів та механізмів забезпечення цілісності і конфіденційності інформації та доступності до неї (рис.3.10).

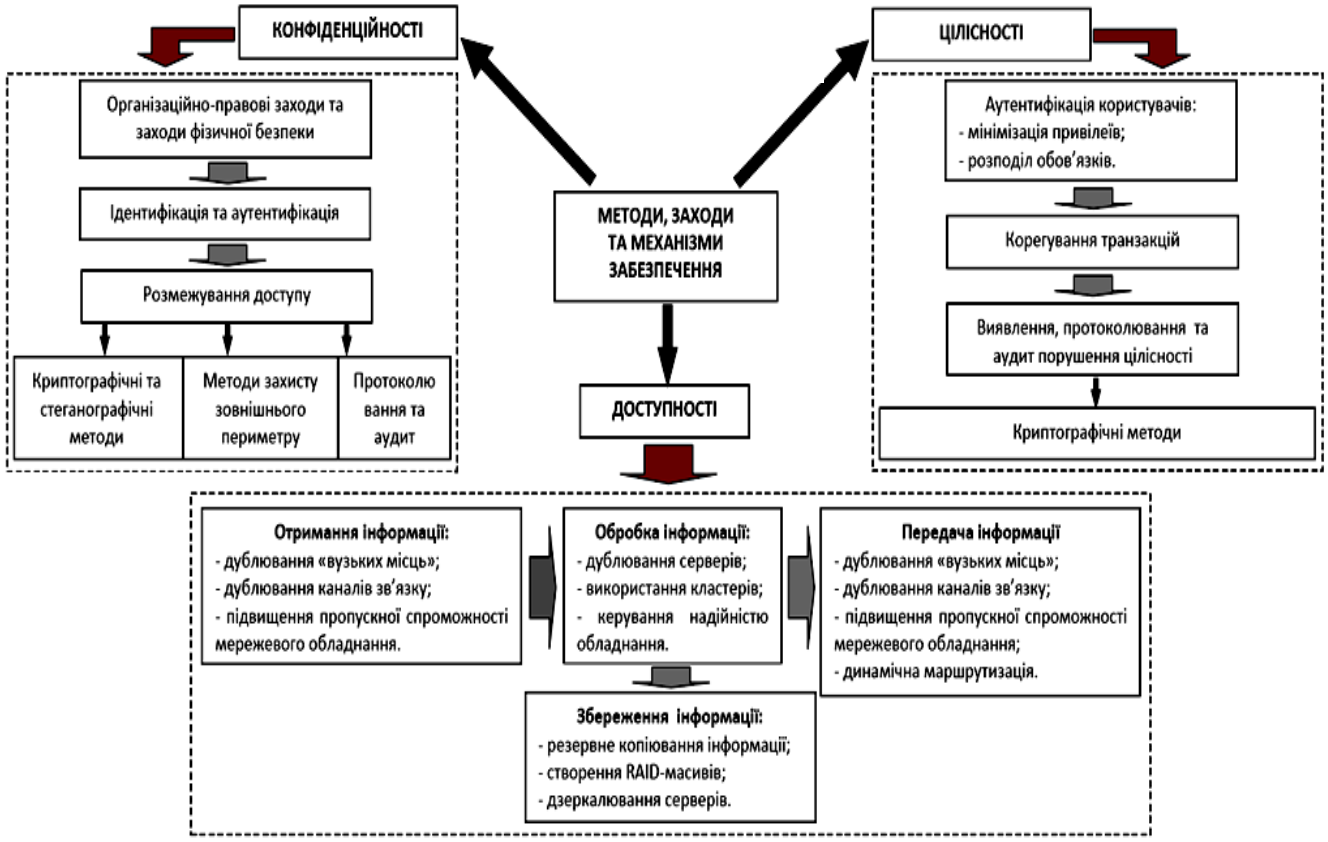


Рис.3.10. Методи, заходи та механізми
забезпечення цілісності і конфіденційності інформації та доступності до неї

Висновки до третього розділу

Захист перспективних АСУ ОКІ може бути реалізований, як відомо, лише за умови розуміння загроз та уразливостей, які таким системам притаманні. Найбільш актуальними серед них експерти останнім часом вважають загрози застосування фішингу, шкідливих програм (вірусів, сніферів, троянів), завідомо фальшивого ПЗ, злоякісних шифруючих кодів, перевантаження та диверсії, а також несанкціонований доступ.

Зважаючи на таке одним із головних завдань при створенні перспективної АСУ ОКІ є формування такої системи безпеки, яка б забезпечувала, *по-перше*, однакову спрямованість завдань безпеки і потреб держави / бізнесу, *по-друге,* ефективне використання ресурсів і зусиль, а також, *по-третє,* сприяла підвищенню вигоди від робіт і заходів безпеки. Саме тому на завершуючому етапі виконання дисертаційної роботи було розроблено та апробовано семантичну модель протиборства системи захисту АСУ ОКІ з атакуючою стороною, а також досліджено вплив шкідливих програм (завідомо фальшивого ПЗ, злоякісних шифруючих кодів) на інформаційні та технологічні процеси процеси в гарантоздатних АСУ ОКІ. Це дозволило, як результат, планувати заходи та обирати раціональні методи щодо відбиття нападу атакуючої сторони та нівелювання його наслідків.

Оскільки наслідком деструктивної роботи шкідливих програм (завідомо фальшивого ПЗ, злоякісних шифруючих кодів) є, як правило, спотворення даних, наприклад, шляхом їх зашифрування, – наступним кроком реалізації розділу стало вирішення завдання щодо детектування та відновлення зашифрованих даних з метою розкриття їх вихідного значення або відновлення секретного ключу, за допомогою якого зашифровані повідомлення були створені. Для вирішення цього завдання в роботі запропоновано спільно з методами криптоаналізу застосовувати методи кластеризації. За рахунок формування деревоподібної ієрархічної структури з N підзадач для розпаралелювання задач/операцій криптоаналізу це дозволило створити передумови для пошуку вразливостей або істинних значень ключів, застосованих для шифрування даних, а також оцінювання стійкості криптосистем.

Стан захищеності обраного варіанту побудови перспективної гарантоздатної АСУ ОКІ від стороннього кібернетичного впливу та загроз, що класифікуються за метою реалізації може бути, як результат, знайдений за допомогою комплексного показника $P_{стан.захищ.}^{K_q^{total}}$ Якщо стан захищеності АСУ ОКІ не відповідатиме технічним умовам та технічному завданню щодо створення системи захисту, то має бути впроваджений комплекс додаткових заходів.

Науково-методичний апарат, викладений в третьому розділі дисертаційної роботи, по-перше, дає можливість підвищити обґрунтованість пропозицій щодо доцільності розробки нових гарантоздатних АСУ ОКІ або проведення модернізації існуючих й, по-друге, може бути розповсюджений на всі об’єкти критичної інфраструктури нашої держави.

Список джерел, використаних у третьому розділі

1. Годин В.В. Управление информационными ресурсами. / В.В. Годин, И.К. Корнеев. - М .: Инфра-М, 1999. - 432 с.
2. Кузнецов И.Н. Информация: сбор, защита, анализ. Учебное пособие по информационно-аналитической работе / И.Н. Кузнецов - М .: Изд. Яуза, 2001. - 246 с.
3. **Kuzmenko L.V.,** Kononenko O.V., Boskin O.O. Features of implementation of the information security policy in the creation of the rational system of electronic documentary cooperation for public and commercial structures of Ukrain. Збірник наукових праць «Системні технології» Національної металургійної академії України. Том 6 (113) 2017, – С. 43–61
4. Адам Тернер. Интернет вещей и носимые технологии : решение тайны частной жизни и безопасности, не сорвать инноваций. – 21 Rich. – JL & Технология. – № 6 (2015), – Режим доступу : http://jolt.richmond.edu/v21i2/article6.pdf;
5. Internet of Things: Privacy & Security in a Connected. – World Federal Trade Commission (FTC) Staff Report. – January 2015. – Режим доступу : https://www.ftc.gov/system/files/documents /reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-priva cy/150127IPrpt.pdf
6. **Кузьменко Л.В.,** Бурячок В.Л. Тенденції розвитку та особливості забезпечення безпеки сучасних IOT-пристроїв. І міжнародна науково-практична конференція «Проблеми кібербезпеки інфрормаційно-телекомунікаційних систем». Збірник матеріалів НПК Київського національного університету імені Тараса Шевченка, 05-06.04.2018. – К.: НУ ТГШ, 2018. – С. 264–268
7. A. Young, M. Yung. Malicious cryptography exposing cryptovirology. Wiley Publishing, Inc., 2004, 392p.
8. Zammis Clark. The worm that spreads WanaCrypt0r. Malwarebytes (12.05.2017). Дата звернення 05.10.2020. Режим доступу: https://blog.malwarebytes.com/threat-analysis/2017/05/the-worm-that-spreads-wanacrypt0r/
9. Гулак Г.М. Уточнена модель порушника та модель реалізації кібератак в системах управління технологічними процесами. / Гулак Г.М., Кащук В.І., Складанний П.М. // IX Всеукраїнська науково-практична конференція «Актуальні проблеми управління інформаційною безпекою держави» (Київ, 30 березня 2018р.): Київ: Нац. акад. СБУ, 2018 – С. 47-49
10. Щербаков А.Ю., Домашев А.В., Прикладная криптография. Использование и синтез криптографических интерфейсов. – М.: Издательско-торговый дом «Русская редакция», 2003, - 416 с.: ил.

11. Гулак Г.М. Оцінка ризиків у ході проведення інженерного аналізу безпеки стеганографічних систем // Сборник научных трудов НАУ. Специальный выпуск , - К.: НАУ, 2008, с. 259-264
12. M. Suiche, WannaCry -Decrypting files with WanaKiwi + Demos. Comae Technologies (19.05.2017). Дата звернення 05.10.2020 Режим доступу: https://blog.comae.io/wannacry-decrypting-files-with-wanakiwi-demo-86bafb81112d
13. Козачок В.А., Рой Я.В., **Бурячок Л.В.** Технології протидії шкідливим програмам та завідомо фальшивому програмному забезпеченню. Сучасний захист інформації. – К.: ДУТ, 2017. – № 2(30). – С. 30–34.
14. Голд Б., Рейдер Ч. Цифровая обработка сигналов. – М.,: «Сов. Радио», 1973, - - 368 с.
15. Бабаш А.В., Шанкин Г.П., Криптография, - М.: СОЛОН-Р, 2002, - 512с.
16. **Бурячок Л.В.** Класифікація соціотехнічних систем за методом кластерізації кількісних даних. «Проблеми кібербезпеки інфрормаційно-телекомунікаційних систем». НТК Київського національного університету імені Тараса Шевченка, 10-11.03.2016. Збірник матеріалів доповідей та тез. – К.: НУ ТГШ, 2016. - С. 24–25.
17. Sokolov V. Development of low-budget spectrum analyzers for IOT and sensor networks. X International conferece of students, PHD- students and young scientists «Engineer of XXI Century». / V. Sokolov, A. Platonenko, **L. Kuzmenko**, V. Buriachok // Projektowanie, badania i eksploatacja. – Bielsku-Białej: NATH, 2020. – P. 331–342. ISBN: 978-83-66249-54-7.
18. Бююль А., Цёфель П. SPSS: Искусство обработки информации. Анализ статистических данных и восстановление скрытых закономерностей. – СПб.: ООО «ДиаСофтЮП», 2002. – 608 с.
19. ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems —Requirements. [Електрон. ресурс]: – Режим доступу: http://www.itgivernance.co.uk/standards.arx.
20. Гавриленко О.В. Відповідність національної нормативної бази у сфері технічного захисту інформації міжнародним стандартам: зіставлення документів, шляхи гармонізації. Матеріали XVII Міжнародної науково-практичної конференції «Безпека інформації у інформаційно-телекомунікаційних системах», м.Київ, 2015.
21. ДСТУ 2938-94 Система оброблення інформації. Основні поняття. Терміни і визначення. [Чинний від 1996-01-01]. Вид. офіц. Київ, Україна: Держстандарт України, 1995.
22. НД ТЗІ 3.7-003-05 “Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі”. [Електрон.

ресурс]: – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=46074&cat_id=38835.

23. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни і визначення. [Чинний від 1998-01-01]. Вид. офіц. Київ, Україна: Держстандарт України, 1997.
24. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. [Чинний від 1999-07-01]. Вид. офіц. Київ, Україна: ДСТСЗІ СБ України, 1999.
25. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. [Чинний від 1999-04-28]. Вид. офіц. Київ, Україна: ДСТСЗІ СБ України, 1999.
26. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу. [Чинний від 2003-04-02]. Вид. офіц. Київ, Україна: ДСТСЗІ СБ України, 2003.
27. НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу "2".[Чинний від 2002-13-12]. Вид. офіц. Київ, Україна: ДСТСЗІ СБ України, 2002.
28. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – 288 с.
29. Козачок В.А., Бурячок В.Л., **Бурячок Л.В.,** Складанний П.М. Пентестінг, як інструмент комплексної оцінки ефективності захисту інформації в розподілених корпоративних мережах. Сучасний захист інформації. – К.: ДУТ, 2015. – № 3. – С. 4–12.
30. Козлов С.Е. Теорія і практика боротьби з комп'ютерною злочинністю /В. О. Козлов. – М.: Гаряча лінія. – Телеком, 2012. — 176 с.
31. Сердюк С.А. Перспективні технології виявлення інформаційних атак/ В. А. Сердюк // Системи безпеки. – 2012. – № 5(47). – С. 96-97.
32. Антимонов Ц.Р. Інтелектуальні протистояння по лінії фронту Вірус-антивірус // Інформація і безпека: матеріали міжрегіональної науково-практ.конф. – Інформація і безпека. – Випуск 2. – Воронеж: ВДТУ, 2012. – С. 39-46.
33. Розподілений антивірусний контроль як спосіб протидії злоякісним програмами в автоматизованих інформаційних системах / С.В. Скриль та ін // Радіосистеми. – Вип. 37 «Радіотехнічні та інформаційні системи охорони і безпеки». – Радіотехніка. – 2014. – №6. – С. 27-30.

34. Мінаєв С.А. Принципи організації протидії шкідливим програмам в інформаційно-телекомунікаційних системах на основі оптимізації їх функціонування / В. А. Мінаєв, С. В. Скриль // Радіосистеми. – Вип. 47 «Радіотехнічні і інформаційні системи охорони і безпеки». – Радіотехніка. – 2013. – №9. – С. 71-72.
35. Нашинець-Наумова А.Ю., В.Л. Бурячок, Н.В. Коршун, О.Б. Жильцов, П.М. Складанний, **Л.В. Кузьменко**. Технологія забезпечення інформаційної і кібербезпеки в закладах вищої освіти України. Електронне наукове фахове видання «Інформаційні технології і засоби навчання» Інституту інформаційних технологій і засобів навчання НАПН України. Том 77, № 4 (2020), – С. 337 – 354 (Цитування в Scopus, WoS)
36. Будько ММ. Методи підвищення захищеності інформаційних ресурсів автоматизованих систем спеціального призначення та оптимізації структур систем їхнього технічного захисту : дис. канд. техн. наук 05.13.21 / Будько Микола Миколайович. - К., 2002. - 162 с.
37. Будько М.М., Василенко В.С., Короленко М.П. Варіант формалізації процесу захисту інформації в комп'ютерних системах та оптимізації його цільової функції // Реєстрація, зберігання і оброб. даних. – 2000. – Т 2, № 2. – С. 73–84.
38. **Бурячок Л.В.**, Бурячок В.Л., Семко В.В. Технологія проведення порівняльного аналізу та оцінювання стану захищеності автоматизованих інформаційних систем. Сучасний захист інформації. – К.: ДУТ, 2016. – № 4. – С. 16–24.
39. Гулак Г.М., Бурячок В.Л., Складаний П.М,. **Кузьменко Л.В.** Криптовірологія: загрози безпеки гарантоздатним інформаційним системам і заходи протидії шифрувальним вірусам. Кібербезпека: освіта, наука, техніка. Том 2. №10 (2020). – С. 6 – 28. ISSN 2663 – 4023

Розділ 4
ДОСЛІДЖЕННЯ ПРОЦЕДУР, РОЗРОБЛЕНИХ В ПРОЦЕСІ ПОБУДОВИ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ДЛЯ СТВОРЕННЯ ПЕРСПЕКТИВНИХ ГАРАНТОЗДАТНИХ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ ОБ'ЄКТАМИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

4.1 Апробація процедури вибору прототипу мережевої інфраструктури ПГ АСУ ОКІ

Як було показано у розділі 2, топологія МІ перспективної гарантоздатної АСУ ОКІ є одною з найважливіших характеристик, що визначає архітектуру мережі в цілому (табл.2.1). Вибір прототипу топології МІ ПГ АСУ ОКІ є наслідком певного компромісного рішення, яке в роботі досягається за критеріями вартості, функціональності та відповідності технічним вимогам стосовно кожної конкретної ситуації, а також показниками, що певним чином характеризують програмно-апаратні засоби та використовуваний інтерфейс з точки зору (табл.2.3)[2, 3]:

обладнання, монтажних робіт, робіт з обслуговування, тощо;

діагностування, масштабованості, гнучкості та універсальності, тощо;

швидкості роботи, захищеності від відмов, тощо.

Отримані в розділі 2 результати порівняльного оцінювання класичних топологій КМ, як приклад, шинної (Y_1), кільцевої (Y_2), зіркової (Y_3) та стільникової (Y_4) за критеріями вибору рішень в умовах невизначеності (рис.2.1), а саме критеріями Вальда, Севіджа та критерієм надзвичайного оптимізму, не дозволили прийняти однозначне рішення щодо того яка з топологій, обраних для порівняння, буде більш раціональною при створенні перспективної гарантоздатної АСУ ОКІ (табл.2.4).

Саме тому в роботі було проведено додаткове дослідження, в основу якого покладено метод МАІ. Схему проведення дослідження приведено на рис.2.2.

За формулою 2.1 було сформовано:

1) матрицю парних порівнянь показників R_i ($i=\overline{1,n}$, $n=10$), приведених у табл.2.3 та використовуваних для оцінювання, наприклад, шинної, кільцевої, зіркової та стільникової топологій (табл.4.1);

Таблиця 4.1

Матриця парних порівнянь показників, що використовуються при оцінюванні топологій КМ

	Кабельна система	Обладнання	Монтаж	Обслуговування	Універсальність	Діагностуваня	Гнучкість	Масштабованість	Швидкість	Відмовостійкість
Кабельна система	1	1	1	0.33	0.2	1	1	0.33	0.11	0.11
Обладнання	1	1	5	0.33	1	1	3	1	0.33	0.2
Монтаж	1	0.2	1	1	0.2	0.33	0.33	0.33	0.14	0.14
Обслуговування	3	3	3	1	0.33	1	1	1	0.33	0.33
Універсальність	5	1	5	3	1	1	5	1	1	1
Діагностуваня	1	1	3	1	1	1	1	0.33	0.11	0.11
Гнучкість	1	1	3	1	0.2	1	1	1	0.33	0.33
Масштабованість	3	1	3	1	1	3	1	1	1	1
Швидкість	9	3	7	3	1	9	3	1	1	1
Відмовостійкість	9	5	7	3	1	9	3	1	1	1

Максимальне власне значення матриці (табл.4.1) становить 11.359. Відповідний їй власний вектор матє вид:

ХВВ = (*0.091, 0.204, 0.074, 0.211, 0.385, 0.144, 0.155, 0.289, 0.540, 0.576*).

Він являє собою вектор локальних пріоритетів показників;

2) матриці парних порівнянь показників R_i $(i=\overline{1,n},\ n=10)$ за кожним із критеріїв K_t $(t=\overline{1,k},\ k=3)$ при оцінюванні топологій Y_i $(i=\overline{1,n}, n=4)$ наприклад, шинної, кільцевої, зіркової та стільникової топологій, також значення їх власних векторів (таблиці 4.2, 4.3 та 4.4 відповідно);

Для кожної із сформованих матриць коефіцієнти відносної узгодженості знаходяться в межах 10 %. Це свідчить про те, що зазначені матриці сформовані правильно й можуть бути використані для подальших розрахунків.

Таблиця 4.2

Формування матриць парних порівнянь для показників забезпечення дешевизни топологій МІ

Забезпечення дешевизни	**Кабельна система**	Шина	Кільце	Зірка	Стільникова	Значення власного вектора		**Монтаж**	Шина	Кільце	Зірка	Стільникова	Значення власного вектора
	Шина	1	2	2	9	0.789		Шина	1	1	2	5	0.671
	Кільце	0,5	1	1	7	0.44		Кільце	1	1	2	4	0.637
	Зірка	0,5	0,5	1	6	0.422		Зірка	0,5	0,5	1	3	0.353
	Стільникова	0,11	0,14	0,17	1	0.073		Стільникова	0,2	0,25	0,33	1	0.136
	Обладнання	Шина	Кільце	Зірка	Стільникова	Значення власного вектора		**Обслуговування**	Шина	Кільце	Зірка	Стільникова	Значення власного вектора
	Шина	1	1	1	3	0.582		Шина	1	0,5	0,11	0.2	0.091
	Кільце	1	1	1	3	0.582		Кільце	2	1	0,2	0.33	0.169
	Зірка	1	1	1	2	0.532		Зірка	9	5	1	2	0.864
	Стільникова	0,33	0,33	0,5	1	0.199		Стільникова	5	3	0,5	1	0.465

Таблиця 4.3

Формування матриць парних порівнянь для показників забезпечення функціональності топологій МІ

Забезпечення функціональності	**Універсальність**	Шина	Кільце	Зірка	Стільникова	Значення власного вектора		**Гнучкість**	Шина	Кільце	Зірка	Стільникова	Значення власного вектора
	Шина	1	0.33	0.11	1	0.104		Шина	1	0.5	0.14	1	0.130
	Кільце	3	1	0.33	3	0.312		Кільце	2	1	0.25	2	0.254
	Зірка	9	3	1	9	0.939		Зірка	7	4	1	7	0.950
	Стільникова	1	0,33	0,11	1	0.104		Стільникова	1	0,5	0,14	1	0.130
	Діагностування	Шина	Кільце	Зірка	Стільникова	Значення власного вектора		**Масштабованість**	Шина	Кільце	Зірка	Стільникова	Значення власного вектора
	Шина	1	0.5	0.11	0.11	0.075		Шина	1	4	2	8	0.810
	Кільце	2	1	0.2	0.2	0.143		Кільце	0.25	1	0,33	3	0.198
	Зірка	9	5	1	1	0.698		Зірка	0.5	3	1	9	0.546
	Стільникова	9	5	1	1	0.698		Стільникова	0.13	0.33	0,11	1	0.075

Таблиця 4.3

Формування матриць парних порівнянь для показників забезпечення відповідності технічним вимогам топологій МІ

Забезпечення відповідності технічним вимогам	**Швидкість**	Шина	Кільце	Зірка	Стільникова	Значення власного вектора
	Шина	1	0,5	0,33	0,33	0,200
	Кільце	2	1	0,5	0,5	0,312
	Зірка	3	2	1	1	0,647
	Стільникова	3	2	1	1	0,647
	Відмовостійкість	Шина	Кільце	Зірка	Стільникова	Значення власного вектора
	Шина	1	1	0,5	0,33	0,263
	Кільце	1	1	0,5	0,33	0,263
	Зірка	2	2	1	1	0,587
	Стільникова	3	3	1	1	0,719

Вектор власних значень матриць, поданих у табл.4.2, 4.3 та 4.4 при цьому матиме вид: BB = (*4.016, 4.016, 4.013, 4.001, 3.987, 3.996, 3.992, 4.069, 4.005, 4.016*).

За формулою 2.2 було обчислено глобальні пріоритети досліджуваних топологій МІ. Він становитиме: $AB^{glpr} = (1.046 \quad 0.678 \quad 3.864 \quad 0.592)$.

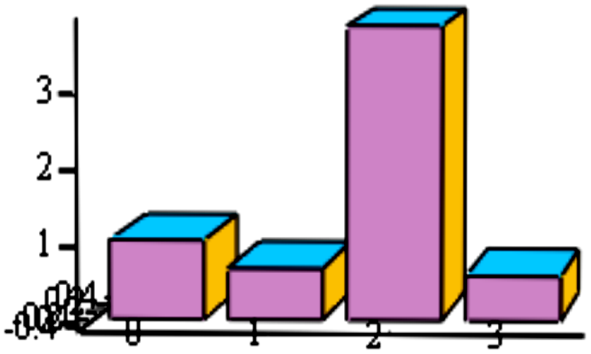


Рис.4.1. Графік порівняння альтернативних топоогій МІ

AB glpr

Враховуючи важливість показників, використовуваних для оцінювання, наприклад, шинної, кільцевої, зіркової та стільникової топологій, найбільш раціональним варіантом при створенні перспективної гарантоздатної АСУ ОКІ може бути топологія типу «зірка»)[3].

Її ваговий коефіцієнт становить:

$AB_{\max}^{glpr} = 3.864$ (рис.4.1)

В подальшому, за результатами експериментальних досліджень (табл. 4.4) з вивчення процесів функціонування запропонованих до розгляду топологій МІ (шинної, кільцевої, зіркової та стільникової) під час рішення задач збору та оцінки даних (інформації), а також прийняття відповідних управлінських рішень за критеріями відносного часу рішення задачі, правильності її рішення та наявності відмов було виявлено, що структурі типу «зірка» порівняно з іншими властива більш висока оперативність та надійність під час рішення задач, сформульованих вище.

Разом з тим було з’ясовано, що топології типу «зірка» характерна найбільша дисперсія часу рішення, що залежить не тільки від змісту задачі, а й від особливостей виконавців. При ускладненні задач зазначеній структурі стають притаманними збільшення відмов та помилкові рішення.

Таблиця 4.4

Результати експериментальних досліджень по вивченню процесів функціонування варіантів топологій МІ

Топологія	Задача	Відносний час рішення задачі, %	Правильність рішення задачі, %	Випадки відмов %
Шина	Збір даних (інформації)	190	60	7
	Оцінка даних (інформації)	140	50	4
	Прийняття управлінського рішення	120	40	4
Кільце	Збір даних (інформації)	130	60	6
	Оцінка даних (інформації)	120	55	3
	Прийняття управлінського рішення	100	45	4
Зірка	Збір даних (інформації)	100	100	2
	Оцінка даних (інформації)	50	70	0
	Прийняття управлінського рішення	30	70	0
Стільникова	Збір даних (інформації)	140	90	4
	Оцінка даних (інформації)	70	90	2
	Прийняття управлінського рішення	50	90	2

Для забезпечення високої швидкості обміну інформацією між комп'ютерами у локальних мережах побудованих за цією топологією слід, враховуючи їх ціну та переваги, вибрати необхідне для цього комунікаційне обладнання. Найкращим рішенням при цьому було б застосування активного обладнання CISCO.

Висновок. Застосування системної процедури ієрархічного представлення елементів перспективної гарантоздатної АСУ ОКІ за критеріями вартості, функціональності і відповідності технічним вимогам з урахуванням місця і внеску показників, що відповідають кожному з цих критеріїв, дозволило створити передумови для організації доступу до мережі та надання обчислювальних ресурсів і послуг їх абонентам для спільного використання IP загального користування, керування їх обміном, передачею, збереженням і поновленням та, на відміну від існуючих, приймати обґрунтовані рішення щодо обрання серед низки можливих варіантів прототипу топології мережевої інфраструктури АСУ ОКІ раціональної структури. Зазначені результати було отримано завдяки застосуванню універсальної системи математичних розрахунків «MATHCAD».

Лістінг підпрограми проведення досліджень наведено у Додатку Б.

Для подальших досліджень, а саме з метою апробації методу формування типового варіанту побудови ПГ АСУ ОКІ вводимо позначення K_{MI}^{nad} та приймаємо, що $K_{MI}^{nad} = AB_{\max}^{glpr}$. В нашому випадку $K_{MI}^{nad} = 3.864$.

4.2 Апробація процедури вибору типового АРМ раціональної конфігурації ПГ АСУ ОКІ

Вирішення задачі щодо вибору типового АРМ раціональної конфігурації для побудови перспективної гарантоздатної АСУ ОКІ, як було показано у розділі 2, обумовлено підвищенням вимог до їх експлуатаційних та технічних характеристик

внаслідок постійного зростання обсягів інформації, що останнім часом обробляється в автоматизованих системах, а також значною вартістю використовуваного в АРМ сучасного високотехнологічного обладнання. Це, в свою чергу, вимагає розробки уніфікованого технічного, математичного, програмного, інформаційного, лінгвістичного, організаційного та інших видів забезпечення АРМ, від якого залежатиме їх продуктивність $P_{prodykt}$. Саме наявність передусім програмно-апаратних видів забезпечення дозволить обрати типовий АРМ, у якому **максимальне значення показника продуктивності** – $P_{prodykt}^{\max}$ буде більшим або дорівнюватиме гранично припустимому значенню даного показника - $P_{prodykt}^{dopyst}$ $\left(P_{prodykt}^{\max} \geq P_{prodykt}^{dopyst}\right)$, а **експлуатаційні витрати** ($C_{експл}$) та **витрати на капітальні вкладення** ($C_{вкл}^{капіт}$) **в уніфікований АРМ** будуть мінімальними)[1, 6].

До переліку основних технічних засобів типового АРМ належать, як відомо, монітор, системний блок, сканер і принтер (багатофункціональний пристрій – БФП), а до програмних – загальне і спеціальне ПЗ. Вартість їх придбання може бути виражена формулою (2.3).

Виходячи з того, що продуктивність кожної складової уніфікованого АРМ може бути виражена лінійною функцією від витрат, які необхідні для їх придбання:

$P_{mnt} = K_1 \cdot C_{mon}$ - показник продуктивності монітора;

$P_{blok}^{syst} = K_2 \cdot C_{blok}^{syst}$ - показник продуктивності системного блоку;

$P_{MFP} = K_3 \cdot C_{MFP}$ - показник продуктивності БФП;

$P_{ZPZ} = K_4 \cdot C_{ZPZ}$ - показник продуктивності ЗПЗ;

$P_{SPZ} = K_5 \cdot C_{SPZ}$ - показник продуктивності СПЗ, -

обчислимо нормуючі коефіцієнти K_1 – K_5, які фактично визначатимуть споживчу ефективність обладнання АРМ і програмного забезпечення, тобто показують взаємозв'язок між вартістю зазначених складових й показниками їх продуктивності: $P_{mon}, P_{blok}^{syst}, P_{MFP}, P_{ZPZ}, P_{SPZ}$.

Для розрахунку зазначених коефіцієнтів необхідно:

на підставі даних виробника та експертних оцінок одержати значення показників продуктивності обладнання і програмного забезпечення, а також цін на них;

враховуючи, що залежність між показниками продуктивності та ціною є величиною лінійною, побудувати апроксимуючу пряму, наприклад, за методом найменших квадратів та обчислити значення цих коефіцієнтів. Вони

дорівнюватимуть котангенсу кута нахилу апроксимуючої прямої до прямої показників продуктивності або надійності обладнання та ПЗ.

Запропонований підхід було досліджено наприкладі розрахунку нормуючого коефіцієнта для можливих конфігурацій системного блоку (СБ) АРМ. Оцінювання СБ проводилось за тактовою частотою процесора (ГГц) та шини (МГц), обсягами ОП (Мб) та HDD (Гб), а також швидкодією HDD (табл.2.6 та 4.5).

Таблиця 4.5

Параметри оцінювання системних блоків та їх значення

№	Тактова частота процесора, ГГц	Тактова частота шини, МГц	Обсяг ОП, Мб	Обсяг HDD, Гб	Швидкодія HDD	Продуктивність %	Ціна, у.о.
1	Athlon XP1 1800+	333	1 x 128 DIMM	40	7200	60	34.9
2	Athlon XP1 2400+	333	512 DDR	80	7200	95	37.8
3	Celeron 433	133	1 x 64 DIMM	10	5400	20	10.5
4	Celeron 633	133	1 x 128 DIMM	10	7200	30	17.1
5	Celeron 1000	233	1 x 128 DIMM	10	7200	40	18.8
6	Celeron 1700	333	1 x 256 DDR	80	7200	55	33.4
7	Celeron 2000	333	1 x 256 DDR	120	7200	60	34.9
8	Celeron 2400	333	1 x 256 DDR	80	7200	60	39.6
9	Celeron 2400	333	1 x 512 DDR	120	7200	70	57.8
10	P 4-1800	533	1 x 256 DDR	120	7200	92	46.6
11	P 4-2000	533	1 x 128 DDR	40	7200	95	37.5
12	P 4-2400	800	1 x 512 DDR	80	7200	100	59.9

Аналіз даних, наведених у табл.4.5, дозволив зробити висновок про те, що одною з кращих (серед оцінюваних) конфігурацій системного блоку є варіант під № 12 – P 4 - 2400. Показник його продуктивності $P_{produkt}$, оскільки він максимальний, було прийнято за 100% й відносно нього обчислено значення показників продуктивності інших конфігурацій СБ АРМ з табл. 4.5. Отримавши їх, було побудовано графік залежності цих показників від відповідних ним значень ціни (рис. 2.6 та 4.2).

Рис. 4.2. Залежність між показниками ціни та продуктивності

За даними графіку, як результат, було визначено котангенс кута нахилу апроксимуючої прямої до прямої показників продуктивності можливих конфігурацій системних блоків АРМ. Для наведеного прикладу він становить:

$K_2 = ctg(6) = 0.26$. Розрахувавши аналогічним чином нормуючі коефіцієнти для багатофункціонального пристрою, загального і спеціального програмного забезпечення ми отримали, що [6]:

$$K_1 = 0.174;\ K_3 = 0.099;\ K_4 = 0.67;\ K_5 = 0.27.$$

Надалі було сформовано цільову функцію, яку необхідно мінімізувати у такий спосіб:

$$F\left(C_{mon}, C_{blok}^{syst}, C_{MFP}, C_{ZPZ}, C_{SPZ}\right) \xrightarrow[v]{} \min,$$

за таких обмежень:

$$P_{dopyst}^{gr} \le K_1 \cdot C_{mon} \le 100,\ P_{dopyst}^{gr} \le K_2 \cdot C_{blok}^{syst} \le 100,\ P_{dopyst}^{gr} \le K_3 \cdot C_{MFP} \le 100$$

$$P_{dopyst}^{gr} \le K_5 \cdot C_{ZPZ} \le 100; \qquad P_{dopyst}^{gr} \le K_6 \cdot C_{SPZ} \le 100;$$

$$C_{mon} > 0 \quad C_{blok}^{syst} > 0 \quad C_{MFP} > 0; \quad C_{ZPZ} > 0; \quad C_{SPZ} > 0 \quad .$$

Зазначені вирази відбивають класичне завдання лінійного програмування, де у якості вхідних даних мають бути задані значення нормуючих коефіцієнтів K_1 – K_5 для всіх складових типового АРМ та гранично припустиме значення показника їх продуктивності ($P_{prodykt}^{dopyst}$). Вирішити його можливо скориставшись можливостями універсальної системи математичних розрахунків «MATHCAD» та виходячи з виділених для цього коштів, визначити оптимально припустимі витрати ($C_{mex+progr}^{APMprip}$) на закупівлю монітора - C_{mon}, системного блоку АРМ раціональної конфігурації - C_{blok}^{syst}, БФП - C_{MFP}, операційної системи - C_{ZPZ} та спеціального програмного забезпечення - C_{SPZ}.

Для цього, позначивши через x_j долю вкладення в j-й ПАЗ, де $j = 1,2,3,4,5$ ми отримали, що чиста приведена вартість інвестицій, наприклад, в закупівлю монітора становитиме $40 \cdot x_1$ у.од., системного блоку – $60 \cdot x_1$ у.од., БФП – $38 \cdot x_3$ у.од., у ЗПЗ – $50 \cdot x_4$ у.од. та у СПЗ– $55 \cdot x_5$ у.од. При цьому слід враховувати, що інвестиції не повинні перевищувати, наприклад, 176 у.од. (табл.4.6).

Таблиця 4.6

Вихідгі дані рішення задачі лінійного програмування

ПАЗ	Чиста приведена вартість, у. од.	Необхідні вкладення, у. од.
Монітор	40	37
Системний блок	60	54
Багатофуунк.пристрій	38	38
Загальне ПЗ (ОС)	50	35
Спеціальне ПЗ	55	51
Виділений обсяг грошових засобів для інвестицій		176

Для того, щоб вибрати один із ПАЗ (або ж навіть деяку їх групу) з найбільшою сукупною чистою приведеною вартістю було складено математичну модель даної задачі. Вона має вид:

$$L(\bar{x}) = 40 \cdot x_1 + 60 \cdot x_2 + 38 \cdot x_3 + 50 \cdot x_4 + 55 \cdot x_5 \to \max$$

при обмеженнях: $37 \cdot x_1 + 54 \cdot x_2 + 38 \cdot x_3 + 35 \cdot x_4 + 51 \cdot x_5 \le 186$.

Причому $x_j = 1$ – ПАЗ фінансується, або $x_j = 0$ – ПАЗ не фінансується.

Вирішивши дану задачу симплексним методом, отримаємо:

$$x_1 = 1;\ x_2 = 1;\ x_3 = 0;\ x_4 = 1;\ x_5 = 1.$$

Як результат, найбільш оптимальним для обладнання АРМ буде фінансування закупівлі монітора (C_{mon}) та системного блоку АРМ (C_{blok}^{syst}), а також операційної системи (C_{ZPZ}) та спеціального ПЗ (C_{SPZ}). Для цього необхідно буде вкласти 177 у.од. (при обсязі, що виділено у 186 у.од.). За такого фінансування чиста приведена вартість проекту комплектування типового АРМ раціональної конфігурації буде максимальною й складе 205 у.од.

Дослідження технології формування експлуатаційних витрат ($C_{експл}$) та додаткових витрат на капітальні вкладення ($C_{вкл}^{капіт}$), а саме витрат на транспортування ($C_{трансп}$), витрат на налагодження ($C_{нал}$) та витрат на запуск ($C_{пуск}$) при виборі типового АРМ раціональної конфігурації в ході роботи експериментально не проводилось. Тому фактично рівень окупності капітальних вкладень на впровадження такого АРМ раціональної конфігурації (2.8) відношенням річної економії від впровадження АРМ(залежатиме від приросту прибутку викликаного, наприклад, зменшенням фонду заробітної плати його користувачів) до витрат на створення типового АРМ (2.3). Згідно проведеного експерименту $K_{\max}^{окупн} = 0.9$.

Тому для подальших досліджень, а саме з метою апробації методу формування типового варіанту побудови ПГ АСУ ОКІ було введено позначення K_{APM}^{eff} та прийнято, що $K_{APM}^{eff} = K_{\max}^{окупн} = 0.9$.

Висновок. Врахування функціональності програмної та апаратної архітектури АРМ, а саме їх системності, гнучкості, стійкості, ефективності, ергономічності, тощо та реалізації нових ІТ у процесах виконання встановлених в АРМ функцій, дозволило забезпечити можливість доступу користувачам до власних і зовнішніх ІР та їх машинної обробки й, на відміну від існуючих, приймати обґрунтовані рішення щодо обрання серед низки можливих АРМ раціональної конфігурації. Це, як результат, дасть можливість користувачам у ході виконання ними посадових

обов'язків оперативно і ефективно реалізовувати власні інформаційні та/або обчислювальні запити. При цьому слід виходити з припущення, що перелік зовнішніх і внутрішніх пристроїв, а також програмного забезпечення уніфікованого АРМ в цьому випадку наведений як приклад і не є достатнім. Його конкретна комплектація визначається місцем АРМ в інформаційному середовищі конкретного ОКІ (установи, підприємства тощо), характером застосування й ступенем її участі в інформаційно-аналітичних процесах.

4.3 Апробація процедури раціонального вибору ПЗ прикладного рівня ПГ АСУ ОКІ

Вирішення задачі щодо вибору ПЗ прикладного рівня ПГ АСУ ОКІ здійснюється в роботі за двома безрозмірними розрахунковими коефіцієнтами функціональності та раціональності. При цьому для порівняльного аналізу, як приклад, було обрано СУБД, оскільки саме ці системи надають можливості щодо створення, збереження, оновлення та пошуку інформації в БД з контролем доступу до даних [https://uk.wikipedia.org/wiki/Система_управління_базами_даних, 4, 5, 11].

В якості досліджуваних було обрано:

СУБД фірми *Oracle* - *Oracle Enterprise Edition* (R_1);

СУБД фірми *IBM* - *DB2* (R_2);

СУБД фірми *Microsof* - *Microsoft SQL Server* (R_3).

Для проведення порівняльного аналізу СУБД в ході експерименту було обрано функції і критерії (варіанти реалізації функцій), що подані в таблиці 2.8.

З використанням методу МАІ було побудовано обернено-симетричні матриці парних порівнянь:

1) функцій F_i^2, де $(i=\overline{1,N},\ N=3)$ $\quad D1:=\begin{pmatrix} 1 & 0.25 & 0.33 \\ 4 & 1 & 2 \\ 3 & 0.5 & 1 \end{pmatrix}$;

2) критеріїв K_{ij}^3 за кожною функцією окремо (якщо $i=1$, то $j=\overline{1,2}$; якщо $i=2$, то $j=\overline{1,5}$; якщо $i=3$, то $j=\overline{1,3}$), що притаманні усім R СУБД:

$$KK1:=\begin{pmatrix} 1 & 4 \\ 0.25 & 1 \end{pmatrix};\qquad KK2:=\begin{pmatrix} 1 & 0.14 & 0.25 & 0.5 & 0.33 \\ 7 & 1 & 3 & 5 & 4 \\ 4 & 0.33 & 1 & 4 & 3 \\ 2 & 0.2 & 0.25 & 1 & 0.5 \\ 3 & 0.25 & 0.33 & 2 & 1 \end{pmatrix};\qquad KK3:=\begin{pmatrix} 1 & 3 & 2 \\ 0.33 & 1 & 0.25 \\ 0.5 & 4 & 1 \end{pmatrix};$$

3) критеріїв K_1^2 - K_{10}^2 між собою:

$$TTX:=\begin{pmatrix} 1 & 2 & 5 & 3 & 0.33 & 0.25 & 3 & 2 & 0.5 & 0.33 \\ 0.5 & 1 & 3 & 2 & 4 & 3 & 2 & 0.5 & 0.33 & 0.25 \\ 0.2 & 0.33 & 1 & 0.5 & 0.25 & 0.33 & 0.2 & 0.16 & 0.14 & 0.25 \\ 0.33 & 0.5 & 2 & 1 & 3 & 5 & 4 & 0.25 & 0.33 & 0.25 \\ 3 & 0.25 & 4 & 0.33 & 1 & 3 & 5 & 0.5 & 0.2 & 0.33 \\ 4 & 0.33 & 3 & 0.2 & 0.33 & 1 & 3 & 0.33 & 0.5 & 0.25 \\ 0.33 & 0.5 & 5 & 0.25 & 0.2 & 0.33 & 1 & 0.16 & 0.2 & 0.14 \\ 0.5 & 2 & 6 & 4 & 2 & 3 & 6 & 1 & 3 & 2 \\ 2 & 3 & 7 & 3 & 5 & 2 & 5 & 0.33 & 1 & 0.14 \\ 3 & 4 & 4 & 4 & 3 & 4 & 7 & 2 & 7 & 1 \end{pmatrix}.$$

4) досліджуваних СУБД за кожним критерієм окремо.

$$A1:=\begin{pmatrix} 1 & 4 & 3 \\ 0.25 & 1 & 2 \\ 0.33 & 0.5 & 1 \end{pmatrix} \quad A2:=\begin{pmatrix} 1 & 0.5 & 0.16 \\ 2 & 1 & 0.33 \\ 7 & 3 & 1 \end{pmatrix} \quad A3:=\begin{pmatrix} 1 & 0.14 & 0.16 \\ 6 & 1 & 0.5 \\ 7 & 2 & 1 \end{pmatrix} \quad A4:=\begin{pmatrix} 1 & 3 & 4 \\ 0.33 & 1 & 2 \\ 0.25 & 0.5 & 1 \end{pmatrix} \quad A5:=\begin{pmatrix} 1 & 0.25 & 0.33 \\ 4 & 1 & 5 \\ 3 & 0.2 & 1 \end{pmatrix}$$

$$A6:=\begin{pmatrix} 1 & 5 & 2 \\ 0.2 & 1 & 0.25 \\ 0.5 & 4 & 1 \end{pmatrix} \quad A7:=\begin{pmatrix} 1 & 0.14 & 0.25 \\ 7 & 1 & 1 \\ 4 & 1 & 1 \end{pmatrix} \quad A8:=\begin{pmatrix} 1 & 2 & 5 \\ 0.5 & 1 & 5 \\ 0.2 & 0.2 & 1 \end{pmatrix} \quad A9:=\begin{pmatrix} 1 & 3 & 2 \\ 0.33 & 1 & 2 \\ 0.5 & 0.5 & 1 \end{pmatrix} \quad A10:=\begin{pmatrix} 1 & 0.33 & 0.25 \\ 3 & 1 & 2 \\ 4 & 0.5 & 1 \end{pmatrix}$$

За результатами опрацювання матриць $KK1$, $KK2$, $KK3$, $D1$, TTX та $A1$ - $A10$ було зроблено висновок про те, що:

<u>*по-перше*</u>, наведені матриці сформовані правильно. Коефіцієнти їх відносної злагодженості знаходяться в інтервалі від 10% до 20% та становлять:

для матриці $D1$ - $OtnSgD1 = 1.326\ \%$;

для матриці $KK1$ - $OtnSgKK1 = 0\ \%$;

для матриці $KK2$ - $OtnSgKK2 = 2.858\ \%$;

для матриці $KK3$ - $OtnSgKK3 = 8.898\ \%$;

для матриці TTX - $OtnSgTTX = 12.88\ \%$

для матриць $A1$ … $A10$:

$OtnSgA =$

	1	2	3	4	5	6	7	8	9	10
1	3.464	1.234	1.196	0.516	6.548	0.825	0.985	1.799	4.473	3.464

<u>*по-друге,*</u> найбільш визначальними при виборі СУБД є функції F_2^2 та F_3^2;

<u>*по-третє,*</u> найбільш визначальним за функцією F_1^2 є критерій K_1^2, за функцією F_2^2 - критерії K_4^2 та K_5^2, та за функцією F_3^2 - критерії K_8^2 та K_{10}^2.

по-четверте, найбільш визначальними критеріями, яким у наборі локальних пріоритетів відповідають максимальні значення та які більшою мірою впливають на вибір раціональної СУБД із сукупності досліджуваних, є критерії K_1^2, K_4^2, K_5^2, K_8^2 та критерій K_{10}^2.

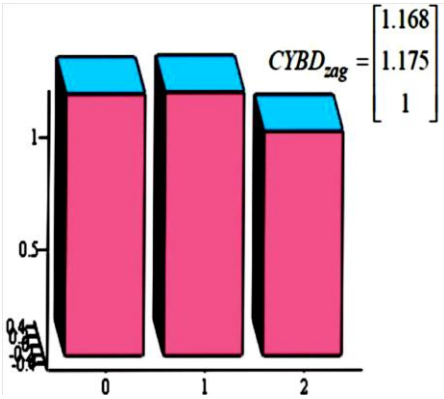
З метою підтвердження цих висновків було побудовано морфологічну карту альтернативних ПЗ(рис.2.8) та позитивно-негативну матрицю (ПНМ) варіантів реалізації функцій ПЗ (R_1, R_2 та R_3), обраних для порівняння (табл.2.9).

Скориставшись результатами бальної оцінки k-го варіанту реалізації i-ї функції якості ПЗ (R_1, R_2 та R_3) наданої незалежними експертами $B_{ik} = (7,\ 2,\ 5,\ 5,\ 9,\ 6.5,\ 4,\ 8,\ 6,\ 9)$, було обчислено нормовані коефіцієнти рівня якості кожної з функцій (табл.2.10) та узагальнюючі показники чотирьох варіантів їх реалізації [8]:

$$K_{ПЗ_1} = 0.114 + 0.091 + 0.091 = 0.296; \qquad K_{ПЗ_2} = 0.114 + 0.141 + 0.018 = 0.273;$$

$$K_{ПЗ_3} = 0.114 + 0.091 + 0.018 = 0.223; \qquad K_{ПЗ_4} = 0.114 + 0.141 + 0.091 = 0.346.$$

Висновок. Найкращим при цьому вважатиметься варіант №4, якому відповідає найбільше значення коефіцієнта $K_{ПЗ}^{\max}$. Для подальших досліджень, а саме з метою апробації методу формування типового варіанту побудови ПГ АСУ ОКІ було введено позначення $K_{ПЗ}^{fynkc}$ та прийнято, що $K_{ПЗ}^{fynkc} = K_{ПЗ}^{\max}$. В нашому випадку $K_{ПЗ}^{fynkc} = 0.346$. Обчисливши глобальні пріоритети отримаємо, що за сукупністю функцій і критеріїв, перелічених у табл.2.12 та з врахуванням, як їх впливу на очікуваний результат, так й суджень абонентів щодо важливості критеріїв кращим серед конкуруючого ПЗ ПР з точки зору раціональності, вважатиметься СУБД *DB2* фірми *IBM* ($ПЗ_{DB2}^{zag} = 1.175$).



Вибір СУБД *DB2* згідно висновків експертів може бути пояснений тим, що зазначена система:

може співпрацювати з усіма програмними платформами, використовуючи при цьому один і той самий код ядра;

на відміну від багатьох інших поставляється як єдине ціле (в СУБД *Oracle* та *MS SQL Server* є окремі компоненти, які потрібно замовляти додатково);

здатна функціонувати в клієнт-серверному режимі (причому і клієнтська, і серверна частини можуть працювати в різних операційних системах).

Важливим фактором на користь вибору СУБД *DB2* може бути й те, що у багатьох організаціях та установах України на цей час накопичений певний досвід роботи із продуктами корпорації *IBM*, зокрема з системою електронного документообігу *Lotus Notes*. За таких обставин СУБД *DB2* може стати, наприклад, логічним розширенням її можливостей. Зазначені результати було отримано завдяки застосуванню універсальної системи математичних розрахунків «MATHCAD». Лістінг підпрограми проведення досліджень наведено у Додатку В.

Для подальших досліджень, а саме з метою апробації методу формування типового варіанту побудови ПГ АСУ ОКІ було введено позначення $K_{ПЗ}^{racion}$ та прийнято, що $K_{ПЗ}^{racion} = ПЗ^{zag}$. В нашому випадку $K_{ПЗ}^{racion} = 1.175$.

4.4 Апробація процедури вибору типового варіанту побудови ПГ АСУ ОКІ

Відомо, що загальний позитивний стан якості будь-якої АСУ може бути охарактеризовано, наприклад, таким чином:

трафік по мережевій службі системи передається надійно з гарантованим захистом як від вірусів, так й від атак порушників;

широкий спектр послуг надається системою безперебійно за гнучкою схемою 24x7, тобто 24 години на добу протягом 7 днів тижня.

Оцінити якість АСУ можливо на підставі часткових критеріїв, обчислених на попередніх етапах роботи (табл.2.15) - $K_{MI}^{nad} = 3.864$, $K_{APM}^{eff} = 0.9$, $K_{ПЗ}^{fynkc} = 0.346$ та $K_{ПЗ}^{racion} = 1.175$. Саме вони найбільш повно характеризують конкретну АСУ з точки зору її топології, архітектури (зокрема АРМ) та ПЗ, а також властивих для неї функцій й дозволяють серед альтернативних обрати типовий, найбільш раціональний варіант побудови ПГ АСУ ОКІ (табл.4.7) [7, 9].

Таблиця 4.7

Оцінка критеріїв і показників якості АСУ, що може бути сформована з використанням результатів попередніх досліджень

Критерій оцінки АСУ	**Вага критерію оцінки** R_i	**Показник критерію**			**Вага показника** γ_{il}	**Розрахункова оцінка показника**			**Комплексна оцінка критерію** $x_{q_{il}}^{j}$	**Нормована вага критерію** $R_{ij}^{нор}$
		Функція, що притаманна показнику	**Міра виміру**	**Шкала виміру**		**Рахункова кількість** η_l	**ідеальна кількість** $\eta_{l_{идеал}}$	**Значення** K_{il}^{j}		
Надійність магістральної МІ	K_{MI}^{nad} = 3.864	***Готовність:*** готовність до роботи обл..лінійного тракту	імовірність	0.1-0.99	3,53	0.95	0,965	0,98	3,53	0,375
		Безперебійність: середній час між відмовами	год.	200-5000		270.1	277,78	0.97		
		Відновлюваність: середній час відновлення	год.	2-100		6	10	0,6		

Функціональність ПЗ	$K_{ПЗ}^{fynkc}$ =0.346	***Доступність***: відносний час працездатного функціонування	імовірність	0.1-0.99	1,36	0,89	0.99	0,89	1,36	0,141
		Змінюваність: тривалість підготовки змін	год.	1-1000		100	150	0,67		
		Замінюваність: тривалість заміни компонентів ПЗ	год.	1-100		82	99	0,82		
Раціональність ПЗ	$K_{ПЗ}^{racion}$ =1.337	***Вивчаємість***: трудомісткість вивчення і застос.ПЗ	чол/год.	1-1000	1,65	100	150	0,67	1,65	0,173
		Адаптованість: трудомісткість адаптації	чол/год.	1-100		97	100	0,97		
		Простота установки: тривалість інсталяції ПЗ	чол/год.	1-100		88	100	0,88		
Ефективність АРМ	K_{APM}^{eff} =0,9	***Відкритість:*** можливість роботи у складі АСУ	порядкова	1-10	2,91	10	10	1,0	2,91	0,311
		Забезпечення єдиного ТК простору: внутрішньо системна інформ.звя'зність	порядкова	1-10	4	8	10	0,8		
		Захищеність: багаторівнева система захисту даних	порядкова	1-10	5	7	10	0,7		

Результат обчислення комплексного показника якості і-го варіанту АСУ подано в таблиці 4.8. За умови порівняння декількох альтернативних варіантів, остаточний вибір серед них типового варіанта побудови буде здійснюватися на підставі наступного правила:

– якщо $K_q^{total} \geq K_{q+1}^{total}$, то q-й варіант АСУ є більше якісним у порівнянні з $q+1$ та навпаки;

– якщо $K_q^{total} = K_{q+1}^{total}$, то варіанти рівнозначні.

Таблиця 4.8

Результат обчислення комплексного показника якості АСУ

Критерій (властивість)			Комплексний показник якості досліджуваної АСУ K_q^{total}, $q=1$
	Нормована вага критерію (властивості) $v_q^{норм}$	Середнє значення вагового коефіцієнта важливості кожного критерію $R_i^{ОПР}/R_i^{нор}$	
Надійність МІ	0.163	0,375	5,61
Функціональність ПЗ	0.325	0,141	
Раціональність ПЗ	0.303	0,173	
Ефективність АРМ	0.209	0,311	

Висновок. Запропонована процедура, як результат, шляхом урахування рівнів впливу кожного критерію на якість функціонування ПГ АСУ ОКІ та чутливості комплексних показників якості при зміні суджень учасників експертної групи, дозволяє обрати серед множини альтернативних рішень раціональний варіант побудови системи, здатний гарантовано надавати необхідні послуги та виконувати потрібні функції в заданих режимах і умовах застосування.

4.5 Апробація процедури детектування та відновлення даних в ПГ АСУ ОКІ

Відомо, що одною із множини можливих зловмисних дій потенційного порушника, спрямованих на дестабілізацію процесів функціонування перспективних гарантоздатних АСУ ОКІ може бути «модифікація або руйнування програмного коду» таких систем або ж «шифрування їх інформаційних ресурсів за допомогою стійких систем шифрування» [10, 12]. Очевидним шляхом шляхом детектування та відновлення зашифрованих ресурсів є застосування методу «грубої сили» для пошуку істинних значень застосованих ключів. В роботі це завдання було вирішене за рахунок розпаралелювання операцій криптоаналізу з використанням технології їх кластеризації.

Апробацію процедури детектування та відновлення даних було проведено для 11 об'єктів $(S=11)$ та п'яти ознак $\left(p=\overline{1,n};\ \ n=5\right)$ по кожному з них. Вихідна вибірка даних та їх нормованих значень може мати вид, що наведений у табл.4.9

Таблиця 4.9

Вхідна вибірка даних та їх нормованих значень

Ознаки / Об'єкти	p_1	p_2	p_3	p_4	p_5
s_1	5	979	3.7	16	0.9
s_2	5	2860	1.8	32	3.4
s_3	5	2669	19.1	3	2.0
s_4	2	2989	6.4	9	0.9
s_5	2	3202	9.4	6	0.7
s_6	6	2668	19.4	3	2.2
s_7	5	2736	2.4	24	3.6
s_8	5	2668	17.4	3	1.9
s_9	5	2670	9.8	6	2.8
s_{10}	2	1005	3.7	16	1.0
s_{11}	2	3953	4.3	14	0.7

Ознаки / Об'єкти	p_1	p_2	p_3	p_4	p_5
s_1	0.8333	0.2477	0.1907	0.5000	0.2500
s_2	0.8333	0.7235	0.0928	1	0.9444
s_3	0.8333	0.6752	0.9845	0.0938	0.5556
s_4	0.3333	0.7561	0.3299	0.2813	0.2500
s_5	0.3333	0.8100	0.4845	0.1875	0.1944
s_6	1	0.6749	1	0.0938	0.6111
s_7	0.8333	0.6921	0.1237	0.7500	1
s_8	0.8333	0.6749	0.8969	0.0938	0.5278
s_9	0.8333	0.6754	0.5052	0.1875	0.7778
s_{10}	0.3333	0.2542	0.1907	0.5000	0.2778
s_{11}	0.3333	1	0.2216	0.4375	0.1944

Матриця близькості (міжточкових відстаней) між об'єктами подана у табл.4.10.

Таблиця 4.10

Міжточкові відстані між об'єктами.

S	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9	s_{10}	s_{11}
s_1	0.4401	0.4629	0.3393	0.3882	0.4818	0.4067	0.4298	0.3628	0.2240	0.4059
s_2	0	0.5950	0.5111	0.5716	0.5976	0.1162	0.5734	0.4148	0.4846	0.4944
s_3		0	0.4034	0.3626	0.0789	0.5234	0.0411	0.2400	0.5098	0.4870
s_4			0	0.0880	0.4617	0.4645	0.3716	0.3390	0.2529	0.1405
s_5				0	0.4268	0.5214	0.3341	0.3489	0.3162	0.1831
s_6					0	0.5249	0.0952	0.2487	0.5572	0.5381
s_7						0	0.5004	0.3199	0.4539	0.4692
s_8							0	0.2120	0.4803	0.4563
s_9								0	0.4181	0.4095
s_{10}									0	0.3370

Побудуємо диполі (пари близько розташованих об'єктів) й поділимо дані на

підвибірки $A \cap B$ і $C \cap D$. Диполі будуються за матрицею близькості об'єктів (табл.. 4.10), причому процедура продовжується доти, поки всі об'єкти увійдуть у множини A і B та C і D.

Як результат одержимо дев'ять диполів для множин A і B:

Адреса диполя	**I**	**II**	**III**	**IV**	**V**	**VI**	**VII**	**VIII**	**IX**
A:	3	3	4	6	2	4	5	8	1
B:	8	6	5	8	7	11	11	9	10

та дев'ять диполів для множин C і D:

Адреса диполя	**I**	**II**	**III**	**IV**	**V**	**VI**	**VII**	**VIII**	**IX**
C:	3	6	4	8	2	11	5	9	1
D:	8	3	5	6	7	4	11	8	10

Побудуємо для них дерева перебору гіпотез про число кластерів. На рис.4.3 подано ієрархічний перебір гіпотез про число кластерів: а - для підвибірки A, б – для підвибірки B. На рис.4.4 – ієрархічний перебір гіпотез про число кластерів: а – для підвибірки C, б – для підвибірки D.

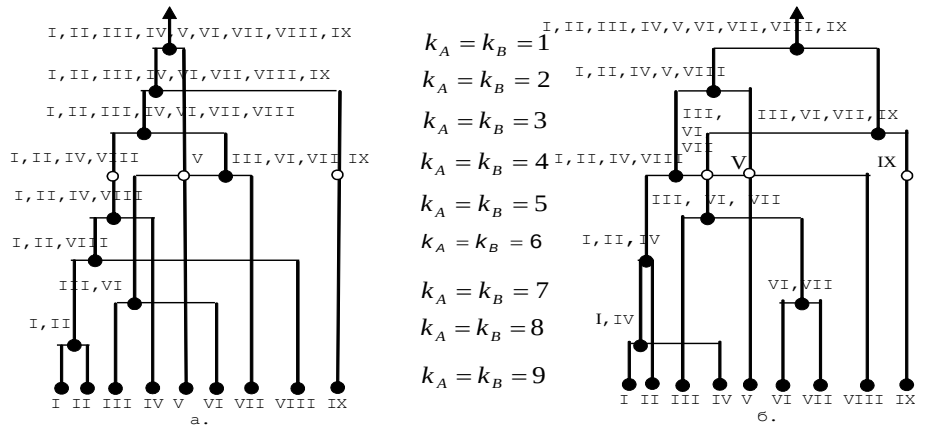


Рис.4.3 - Ієрархічний перебір гіпотез про число кластерів:
а - для підвибірки A, б – для підвибірки B

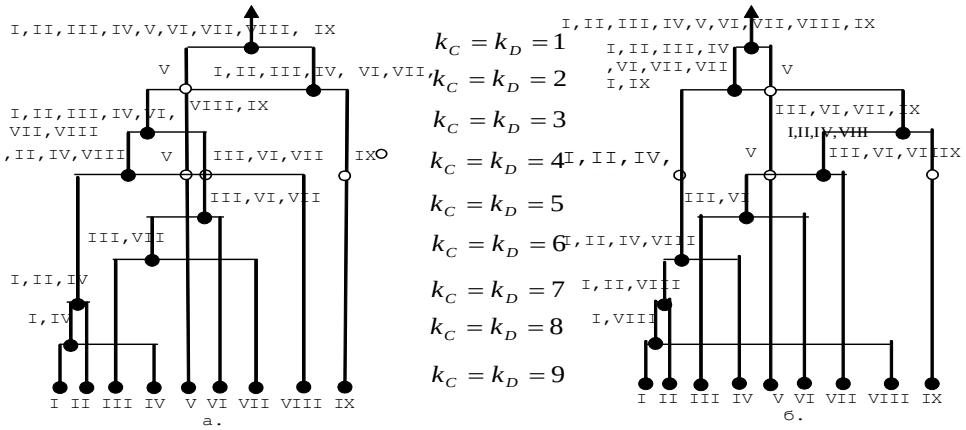


Рис.4.4 Ієрархічний перебір гіпотез про число кластерів:
а - для підвибірки C, б – для підвибірки D

Перебір кластеризацій за сумарним критерієм несуперечності подано у табл.4.11.

Таблиця 4.11

Результати перебору кластеризацій

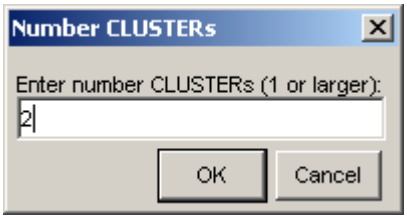
Адреса	Диполя	Об'єкти, об'єднані в кластер	Номер кластера
I II VIII IV	3-8 3-6 8-9 6-8	3,6,8,9	I
V	2-7	2,7	II
III VI VII	4-5 4-11 5-11	4,5,11	III
IX	1-10	1,10	IV

Після проведених розрахунків видно, що оптимальній кластеризації відповідатимуть випадки, коли при $k_A = k_B = k_C = k_D = 4$ сумарний критерій несуперечностя дорівнюватиме нулю.

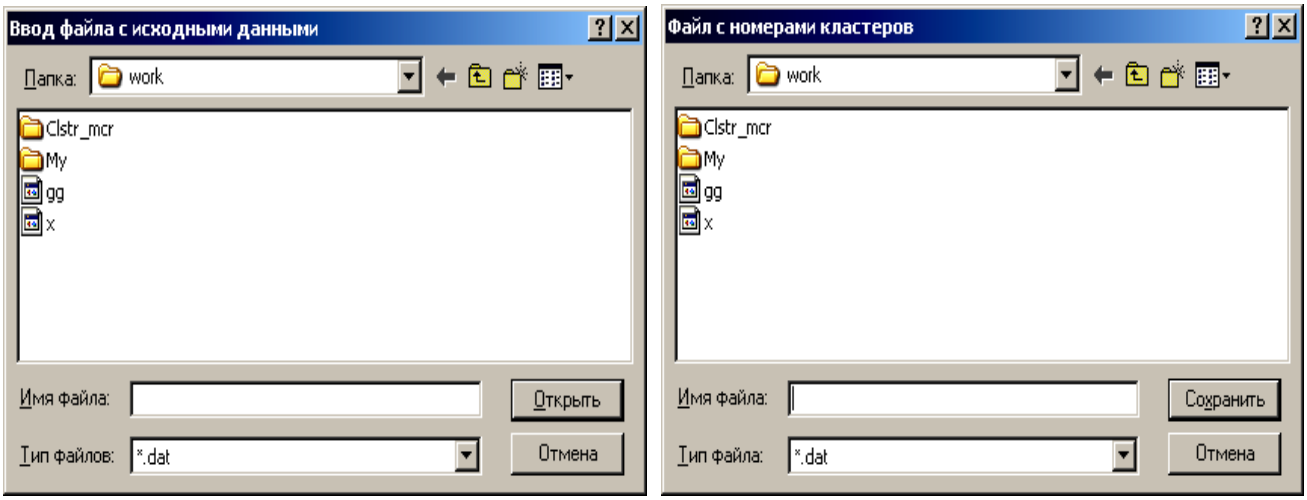
Програма для персональної обчислювальної машини, що реалізує наведений вище алгоритм «Кластер» була розроблена та відлагоджена у математичному середовищі MATLAB v.7.1 в операційної системі WINDOWS XP Pro Serves Pack 2. Для підвищення швидкості її виконання, програму було відкомпільовано внутрішнім компілятором MATLAB v.7.1 у виконавчий файл «Кластер.exe».

Кроки виконання програми «Кластер.exe» зводяться до наступного:

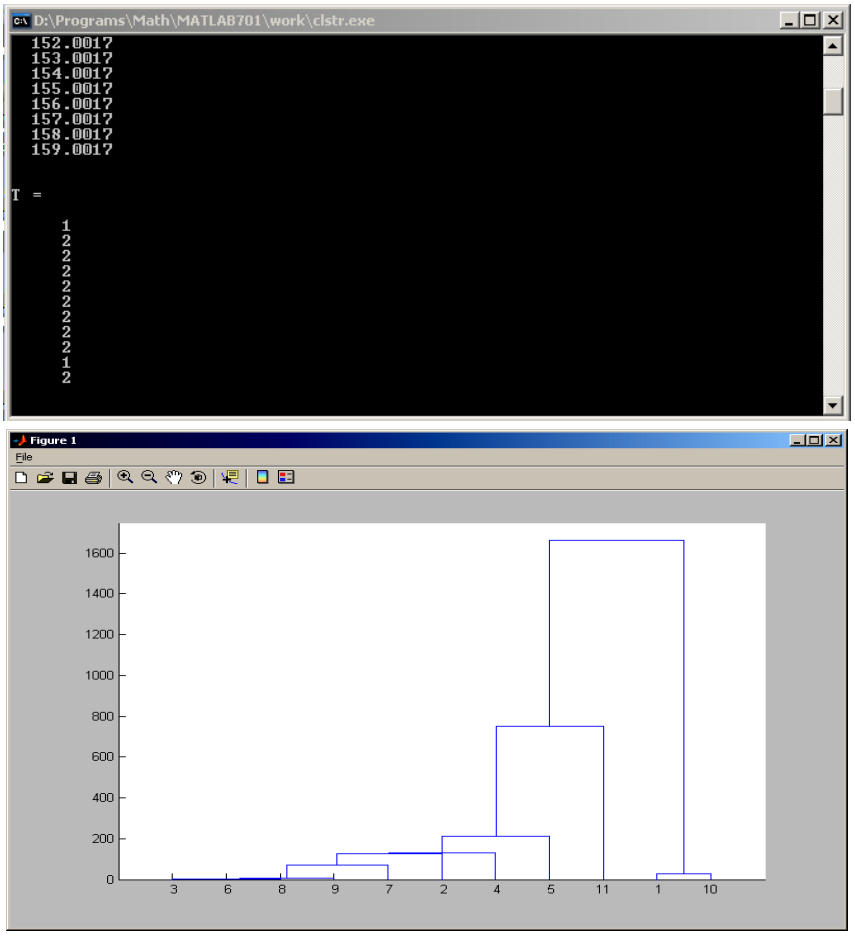
1. Після запуску програми, виводиться запит щодо кількості кластерів, на яку потрібно розбити масив вихідних даних (за умовчуванням 2):



2. Проводиться запит про файл вихідних даних та назву файлу даних, що будуть розраховані (файл з номерами кластерів) у стандартному вікні WINDOWS:



3. Проводяться розрахунки, згідно з алгоритмом кластерізації кількісних даних та виводиться дендрограма кластерів:



Висновок. Запропонована процедура, як результат, дозволяє шляхом кластерізації кількісних даних багатовимірних об'єктів обгрунтувати класифікацію та провести їх порівняльний аналіз. Впровадження процедури в загальний процес визначення впливу загроз на процеси функціонування ПГ АСУ ОКІ створило передумови для пошуку вразливостей або істинних значень ключів, застосованих для шифрування даних, а також оцінювання стійкості криптосистем в умовах впливу шкідливих програм, фальшивого ПЗ і злоякісних шифруючих кодів на інформаційно-технологічні процеси в АСУ ОКІ.

Список джерел, використаних у четвертому розділі

1. Dreis Y. A tuple model for estimating the consequences of personal data leakage in automated systems. VIII International conferece of students, PHD-students and young scientists «Engineer of XXI Century» /Y.Dreis, I.Lozova, A.Biskupskyi, **L.Kuzmenko**, Ali .T. Al-Khwalde, A.Korchenko // Processing, transmission and security of information. – Bielsku-Białej: NATH, 2018. Vol.2. – P. 41–50. ISBN: 978-83-65182-94-4.
2. Sokolov V. Development of low-budget spectrum analyzers for IOT and sensor networks. X International conferece of students, PHD- students and young scientists «Engineer of XXI Century» /V. Sokolov, A.Platonenko, **L.Kuzmenko**, V.Buriachok // Projektowanie,

badania i eksploatacja. – Bielsku-Białej: NATH, 2020. – P. 331–342. ISBN: 978-83-66249-54-7.

3. Рейш О.Е., Бурячок В.Л., Вертегел С.Г., **Бурячок Л.В.** Методика вибору раціональної топології комп'ютерної мережі перспективних автоматизованих систем управління військами. Труди Академії. – К.: НАО МО України, 2009. – № 2(89). – С. 81–90.
4. Бурячок В.Л., **Бурячок Л.В.** Алгоритм порівняльного оцінювання програмних засобів однакового функціонального призначення для розв'язання завдань інформаційної діяльності. Збірник наукових праць. – К.: НДІ ГУР МО України, 2010. Вип. 27. – С. 124–139.
5. Бурячок В.Л., **Бурячок Л.В.,** Костюк Т.Я. Формування набору показників для оцінювання якості програмного забезпечення сучасних автоматизованих систем. Збірник наукових праць. – К.: НДІ ГУР МО України, 2010. Вип. 28. – С. 111–124.
6. Бурячок В.Л., **Бурячок Л.В.,** Гулак Г.М. Алгоритм вибору АРМ раціональної конфігурації. Сучасний захист інформації. – К.: ДУІКТ, 2011. – № 2. – С. 85–94.
7. Бурячок В.Л., **Бурячок Л.В.,** Костюк Т.Я. Обґрунтування вибору раціональної системи електронного документообігу для державних структур спеціального призначення. Вісник воєнної розвідки. – № 24. – 2011. – С. 67–74.
8. **Бурячок Л.В.** Стратегія обґрунтування раціонального набору параметрів і функцій програмних засобів спеціального призначення, спрямованих на розв'язання завдань інформаційної діяльності. Сучасний захист інформації. – К.: ДУТ, 2016. – № 3. – С. 3–9.
9. **Бурячок Л.В.,** Бурячок В.Л., Семко В.В. Технологія проведення порівняльного аналізу та оцінювання стану захищеності автоматизованих інформаційних систем. Сучасний захист інформації. – К.: ДУТ, 2016. – № 4. – С. 16–24.
10. Гулак Г.М., Бурячок В.Л., Складаний П.М,. **Кузьменко Л.В.** Криптовірологія: загрози безпеки гарантоздатним інформаційним системам і заходи протидії шифрувальним вірусам. Кібербезпека: освіта, наука, техніка. Том 2. №10 (2020). – С. 6 – 28. ISSN 2663 – 4023
11. Бурячок В.Л., **Бурячок Л.В.,** Боголій С.М. Порівняльне оцінювання програмних засобів однакового функціонального призначення. «Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення». V-а НТК ВІТІ НТУУ "КПІ" МО України, 20–21.10.2010 р.. Доповіді та тези доповідей. – К.: ВІТІ НТУУ "КПІ", 2010. – С. 75–76.
12. **Бурячок Л.В.** Класифікація соціотехнічних систем за методом кластерізації кількісних даних. «Проблеми кібербезпеки інфформаційно-телекомунікаційних систем». НТК Київського національного університету імені Тараса Шевченка, 10-11.03.2016. Збірник матеріалів доповідей та тез. – К.: НУ ТГШ, 2016. – С. 24–25.

ВИСНОВКИ

Ситуація, що останнім часом спостерігається в світі, характеризується:

вибуховим зростанням обсягів IP, до якого отримали доступ пересічні громадяни;

винайденням потужних комп'ютерів і вбудованих мікроконтролерів, що сприяло розвитку промисловості;

суттєвим збільшенням кількості загроз та їх зростаючою ефективністю;

значним браком кваліфікованих фахівців у сфері безпеки, зокрема інформаційної та кібернетичної.

Прикладом такому може бути: збільшення порівняно з 2015 роком майже на 65% кількості зломів акантів; викрадення внаслідок зломів понад 2,5 мільярдів незахищених записів; потерпання від стороннього кібернетичного впливу кожної п'ятої організації/установи; збільшення середньої тривалості кібератак та часу коли вони залишаються непоміченими; нехтування понад 60% організацій / установ актуальним питанням щодо збільшення видатків на навчання персоналу методам та засобам безпеки, а також способам їх застосування; відсутність у кожного третього фахівця з безпеки знань із реалізації складних APT-атак; відсутність у понад 95% випускників IT сфери банальних знань у IT-галузі, тощо.

Такий стан справ обумовлює необхідність:

по-перше, убезпечення державами світу ІКТ та ІТС, а також захисту ними власної критичної інфраструктури від внутрішніх і зовнішніх втручань та загроз, що реалізуються зловмисниками передусім через атаки нульової доби, атаки на провайдерів, атаки на мобільні пристрої тощо;

по-друге, пошуку серед відомих технологій більш сучасних підходів, які б дозволили створювати перспективні й захищені від стороннього кібернетичного впливу інформаційні системи, зокрема такі, як АСУ ОКІ. При цьому безпека таких систем має бути тісно інтегрованою до об’єкта безпеки – ОКІ, об’єктом захисту в них мають бути інформаційні та технологічні процеси, а не інформація / інформаційний ресурс й, найголовніше, забезпечення цілісності та доступності функцій в таких системах має бути найбільш пріоритетним завданням порівняно із забезпеченням конфіденційності в бізнесі.

Саме ці питання й було досліджено в рамках даної дисертаційної роботи. Результатом її виконання є вирішення актуальної наукової задачі із **розроблення теоретичних і прикладних засад побудови інформаційної технології для** *створення перспективних гарантоздатних АСУ ОКІ,* а також *визначення впливу на процеси функціонування таких систем антропогенних і техногенних втручань та загроз*.

У процесі виконання дисертаційної роботи отримано такі наукові результати.

1. ***Метод формування типового варіанту побудови перспективної гарантоздатної АСУ,*** що поєднує в собі такі базові процедури, як:

процедура вибору прототипу топології мережевої інфраструктури;

процедура вибору типового АРМ раціональної конфігурації;

процедура раціонального вибору ПЗ прикладного рівня, - що в інтересах створення перспективної АСУ забезпечило доступ до мережі та надання обчислювальних ресурсів і послуг її абонентам для спільного використання ними власних і зовнішніх ІР, забезпечило доступ користувачам до таких ІР, керування їх обміном, передачею та машинною переробкою, дозволило автоматизувати процеси пошуку і збору інформації у зовнішніх і внутрішніх джерелах, її реєстрації, трансформації та функціональної обробки, а також процеси захисту ІР в АСУ від кібернетичних загроз.

Комплексним рішенням в межах даного методу, вхідними даними для якого є критерії, що найбільш повно характеризують конкретну АСУ ОКІ з точки зору її топології, архітектури та ПЗ, а також властивих для неї функцій й значення яких було отримано на попередніх етапах роботи, а прийняття рішення щодо вибору раціонального варіанту здійснюється при цьому за безрозмірним показником якості $K_q^{total} = \max$ - є *процедура вибору раціонального варіанту побудови ПГ АСУ ОКІ. Її застосування дозволить ПГ АСУ ОКІ, як результат,* якісно задовольняти потреби користувачів у поданні повної і достовірної інформації та її ефективної обробки, а також гарантовано надавати необхідні послуги/сервіси та виконувати потрібні функції в заданих режимах і умовах застосування.

2. ***Метод визначення впливу загроз на процеси функціонування перспективних гарантоздатних АСУ ОКІ,*** який ґрунтується на моделі загроз безпеці автоматизованих систем та поєднує в собі такі базові моделі та процедури, як:

семантична модель протиборства системи захисту АСУ ОКІ та атакуючої сторони;

процедура детектування та відновлення даних в АСУ ОКІ, - що в інтересах створення перспективної АСУ забезпечило відслідковування стороннього кібернетичного впливу на інформаційні і технологічні процеси ОКІ, а також пошуку вразливостей або істинних значень ключів шифрування даних та оцінювання стійкості криптосистем.

Комплексним рішенням в межах розробленого методу є *модель оцінки стану захищеності перспективної гарантоздатної АСУ ОКІ від загроз порушення цілісності, конфіденційності та доступності* яка, на відміну від подібних, дозволяє оцінювати події, що можуть впливати на інформаційно-технологічні процеси ОКІ та прямо або опосередковано завдати збитку її власникам і користувачам, приймати обґрунтовані

рішення щодо стану захищеності АСУ ОКІ від впливу кібернетичних атак за комплексним безрозмірним показником $P_{стан.захищ.}^{K_q^{total}}$ та, як результат, убезпечити АСУ ОКІ від НСД до її ресурсів та інформації, що в ній циркулює.

3. Розроблено програмні додатки для проведення імітаційних експериментів.

Як наслідок, отримані в роботі наукові результати, утворюють у своїй сукупності ***інформаційну технології для створення перспективних гарантоздатних АСУ ОКІ***, впровадження якої, на відміну від існуючих, забезпечує гарантоване надання абонентам необхідних послуг та/або сервісів, яким в заданих режимах і умовах застосування з урахуванням стану захищеності таких систем від загроз порушення ЦКД можливо виправдано довіряти.

Впровадження означеної ІТ для створення ПГ АСУ ОКІ на прикладі НЕК «Укренерго» окрім всього сприяє (Акт впровадження від 04.01.2021 року):

по-перше, підвищенню ефективності дій осіб, відповідальних за забезпечення безпеки ПГ АСУ ОКІ (за рахунок оперативного визначення найбільш значимих загроз та своєчасного реагування на стан захищеності АСУ від загроз порушення ЦКД) приблизно на 12%;

по-друге, скороченню часу на прийняття виважених управлінських рішень щодо побудови ПГ АСУ ОКІ з відповідним ПАЗ та її впровадженні приблизно на 18 - 20%.

ДОДАТКИ

Додаток А

Формалізована модель загроз АСУ ОКІ (повна)

№ з/п	Тип загрози	Джерело загрози	Можливий метод (спосіб) реалізації атаки	Наслідки		
				К	Ц	Д
1	**Загрози витоку інформації технічними каналами**					
1.1	Загрози витоку акустичної (мовної) інформації					
1.1.2	Несанкціоноване внесення змін в комплекс технічного захисту, ПЗ та компоненти інформаційного забезпечення	Апаратура, Персонал, Користувачі	Недостатній контроль		+	+
1.1.1	Загрози застосування закладних передавальних пристроїв ("жучків"), направлених мікрофонів та стетоскопів	Персонал, Користувачі	Недостатній контроль	+		+
1.1.2	Загрози лазерного та/або інфрачервоного зондування віконних стекол	Персонал, Користувачі	Недостатній контроль	+		+
1.2	Загрози витоку видової інформації					
1.2.1	Загрози порушення технології введення / виведення видової інформації. Копіювання вихідних документів, магнітних та інших носіїв інформації	Персонал, користувачі	Неуважність, недбалість, некомпетентність	+	+	+
1.2.2	Загрози застосування фізичними особами портативної розвідувальної апаратури, що розміщується в транспортних засобах поруч з ОІД або безпосередньо на самому об'єкті	Апаратура, Персонал, Користувачі	Недотримання організаційних заходів	+		
1.2.3	Загрози використання оптичних засобів, дистанційне фотографування тощо для копіювання інформації	Апаратура, Персонал, Користувачі	Недотримання організаційних заходів	+		
1.2.4	Загрози читання видової/залишкової інформації («сміття»), що виводиться на екран, роздруковується або зберігається на запам'ятовуючих пристроях	Персонал, Користувачі	Знаходження в службових приміщеннях сторон.осіб	+		
1.2.5	Загрози розкрадання магнітних носіїв та документів, отримання не облікованих копій	Апаратура, Програми, Персонал, Користувачі	Отримання сторонніми особами доступу до мережевих накопичувачів інформації	+		
1.3	Загрози витоку інформації каналами ПЕМВіН					
1.3.1	Збір за допомогою спеціальних засобів ЕМ випромінювань АСУ (пристроїв відображення інформації, процесорів, ліній зв'язку тощо)	Апаратура	Каналами побічних ЕМВ і наведень	+		
1.3.2	Збір за допомогою спеціальних засобів побічних наведень на доп.засоби та системи (мережі теплопостачання, системи вентиляції, шини заземлення, мережі живлення тощо)	Апаратура	Каналами побічних ЕМВ і наведень	+		
1.3.3	Незаконне підключення до апаратури АСУ, систем електроживлення та заземлення	Апаратура, Персонал, Користувачі	Каналами побічних ЕМВ і наведень	+	+	+
1.3.4	Використання закладних і дистанційних підслуховуючи пристроїв	Апаратура, Персонал, Користувачі	Каналами побічних ЕМВ і наведень	+		
1.3.5	Прослуховування телефонних розмов	Апаратура, Персонал, Користувачі	Каналами ПЕМВіН Несанкціоноване підключення	+		
2	Загрози НСД до інформації, що обробляється на АРМ					
2.1	Загрози, пов'язані з діями порушників доступу до інформації					
	Зміна умов фізичного середовища: аварії, стихійні лиха	Оточуюче середовище	Стихійні лиха, кліматичні зміни		+	+
	Тимчасова відсутність персоналу (хвороба, відрядження, відпустка)	Персонал, користувачі	Сімейні обставини, епідемії, службова необхідність тощо		+	+

	Порушення порядку зберігання та обліку документів, носіїв інформації, даних, технічних засобів	Персонал, користувачі	Неуважність, недбалість, некомпетентність	+	+	+
2.1.1	Загрози, що виникають при завантаженні ОС					
	Загрози, пов'язані з неможливістю працювати із системою через відсутність відповідної підготовки	Персонал, користувачі	Некомпетентність	+	+	
	Загрози, пов'язані з неможливістю працювати із системою через відсутність технічної підтримки (неповнота документації, нестача довідкової інформації тощо)	Персонал, користувачі	Неуважність, недбалість	+		+
	Загрози, пов'язані з порушенням роботи (випадкове або навмисне) систем зв'язку, електроживлення, водо- і/або теплопостачання, кондиціонування	Персонал, користувачі	Неуважність, недбалість, некомпетентність			+
	Загрози, пов'язані з руйнуванням або пошкодженням приміщень	Персонал, користувачі Стих.лиха	Стихійні лиха, кліматичні зміни	+	+	+
2.1.2	Загрози, що реалізуються після завантаження ОС					
	Загрози поширення файлів, що містять несанкціонований виконуваний код у вигляді елементів ActiveX, Java-аплетів, інтерпретованих скриптів (наприклад, текстів на JavaScript)	Хакери Персонал, користувачі	Неуважність, недбалість, некомпетентність	+		+
	Загрози використання недоліків програм, що реалізують мережеві сервіси (зокрема, відсутність контролю за переповненням буфера) на кшталт «вірусу Морріса»	Хакери	Некомпетентність		+	+
	Загрози віддаленого управління системою, що надаються прихованими компонентами («троянськими» програмами типу Back. Orifice, Net Bus), або штатними засобами управління і адміністрування комп'ютерних мереж (Landesk Management Suite, Managewise, Back Orifice і т.п.)	Хакери	Несанкціоноване підключення	+	+	+
2.1.3	Загрози впровадження злоякісних програм					
	Загрози застосування програмних вірусів (включення в ПЗ програмних закладок типу «бомби», «троянського коня» тощо)	Програми, Персонал, Користувачі	Використання неперевіреного ПЗ	+	+	+
	Загрози застосування програмних закладок (недоліки у мовах програмування, операційних системах тощо)	Програми, Персонал, Користувачі	Використання неперевіреного ПЗ	+	+	+
	Загрози впровадження і застосування забороненого політикою безпеки ПЗ (неліцензійного) або несанкціоноване використання ПЗ	Програми, Персонал, Користувачі	Використання не ліцензійного ПЗ	+	+	+
2.2	Загрози інформації із зовнішніх мереж					
2.2.1	Загрози аналізу мережевого трафіку					
	Загрози перехоплення потоку даних, що передаються, якими обмінюються компоненти мережевої ОС	Персонал	Недостатній контроль		+	+
	Загроза відповідності подій, що відбуваються в системі та команд, які передаються цими хостами	Персонал	Недостатній контроль		+	+
2.2.2	Загрози сканування ОС, портів, служб тощо					
	Загрози впровадження і застосування програм, які не є необхідними для виконання службових обов'язків та не передбачені відповідними розпорядчими документами	Персонал, користувачі	Неуважність, недбалість, некомпетентність	+	+	+
	Загрози застосування BrowSerHijackers-програм, здатних замінити початкову	Персонал, користувачі	Неуважність, недбалість, некомпетентність	+	+	+

	сторінку (сторінку, яка запитується), іншими сторінками, які користувач не запитував					
2.2.3	Загрози виявлення паролів					
	Загрози здійснення заходів, що можуть призвести до розголошення паролю адміністратора АСУ або до його втрати, тощо	Персонал, користувачі	Неуважність, недбалість, некомпетентність		+	+
	Загрози здійснення заходів, що можуть призвести до відмови АСУ, руйнування програмно-апаратних та інформаційних ресурсів	Персонал, користувачі	Неуважність, недбалість, некомпетентність		+	+
	Загрози здійснення заходів в автоматизованому (вручну користувачем), або автоматичному режимах, що можуть призвести підбору пароля BIOS	Персонал, користувачі	Недостатній контроль	+		+
2.2.4	Загрози підміни довіреного об’єкту					
	Загрози одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача (“маскарад”).	Програми, Персонал, Користувачі	Отримання сторонніми особами доступу до ресурсів АСУ	+	+	+
	Загрози «імітації дій користувача» та виконанні операцій прийому/передавання даних від його імені	Апаратура, Програми, Персонал, Користувачі	Підключення порушника до обчислювальної мережі та отримання відомостей про конфігурацію мережевих пристроїв, тип ПЗ	+		
2.2.5	Загрози типу «відмова в обслуговуванні»					
	Загрози застосування Mac-flooding – програми, яка підмінює MAC-адресу відправника та/або отримувача інформації на комутатор	Персонал, користувачі	Отримання доступу інформації	+	+	+
	Загрози застосування Форк-бомб – програм, які постійно створюють власні копії	Персонал, користувачі	Отримання доступу інформації	+	+	+
	Загроза застосування XML-бомб – XML документів, які містять багато байтів, символів тощо	Персонал, користувачі	Отримання доступу інформації	+	+	+
	Загрози розсилки великої кількості пакетів	Хакери	Отримання доступу доінформації		+	+
	Загрози перехоплення IP	Хакери	Отримання доступу ресурсів АСУ		+	+
2.2.6	Загрози віддаленого запуску додатків					
	Загрози поширення файлів, що містять несанкціонований виконуваний код	Хакери Персонал	Отримання доступу інформації та ресурсів АСУ			
	Загрози віддаленого запуску програми шляхом переповнення буфера додатків-серверів	Хакери Персонал, користувачі	Отримання доступу інформації та ресурсів АСУ			
	Загрози віддалений запуск програми шляхом використання можливостей віддаленого управління системою	Хакери Персонал, користувачі	Отримання доступу інформації та ресурсів АСУ			
2.2.7	Загрози впровадження злоякісних програм					
	Загрози застосування програм, що використовують не декларовані можливості програмного та програмно-апаратного забезпечення АСУ					
	Загрози застосування програм, що генерують комп’ютерні віруси					
	Загрози застосування програм, що виявляють уразливості засобів захисту інформації в АСУ					

*** НАСЛІДКИ: К – порушення конфіденційності;
Ц – порушення цілісності;
Д – порушення доступності

Додаток Б

Лістинг програми розташування топологій сучасних структурованих компьютерних мереж (СКМ) у ряд переваг

ORIGIN:= 1

Розташування топологій сучасних структурованих компьютерних мереж (СКМ) у ряд переваг.

IsogA := 0.9 індекс випадкової узгодженості матриць розміром 4x4

IsogB := 1.49 індекс випадкової узгодженості матриць розміром 10x10

Nekc := 3 Кількість експертів

Ntm := 4 Кількість досліджуваних топологій сучасних СКМ

Досліджувані топології мереж:
1 - топологія "шина" 3 - топологія "зірка"
2 - топологія "кільце" 4 топологія "стільникова"

Показники за якими порвнюються топології сучасних СКМ (розташовані у порядку їх важливост

Nttx := 10 A10 - відмовостійкість A2 - обладнання
A9 - швидкість A7 - гнучкість
A5 - универсальність A6 - діагностування
A8 - масштабованість A1 - кабельна система
A4 - обслуговування A3 - монтаж

$$A1 := \begin{pmatrix} 1 & 2 & 2 & 9 \\ 0.5 & 1 & 1 & 7 \\ 0.5 & 1 & 1 & 6 \\ 0.11 & 0.14 & 0.17 & 1 \end{pmatrix} \quad A2 := \begin{pmatrix} 1 & 1 & 1 & 3 \\ 1 & 1 & 1 & 3 \\ 1 & 1 & 1 & 2 \\ 0.33 & 0.33 & 0.5 & 1 \end{pmatrix} \quad A3 := \begin{pmatrix} 1 & 1 & 2 & 5 \\ 1 & 1 & 2 & 4 \\ 0.5 & 0.5 & 1 & 3 \\ 0.2 & 0.25 & 0.33 & 1 \end{pmatrix} \quad A4 := \begin{pmatrix} 1 & 0.5 & 0.11 & 0.2 \\ 2 & 1 & 0.2 & 0.33 \\ 9 & 5 & 1 & 2 \\ 5 & 3 & 0.5 & 1 \end{pmatrix}$$

$$A5 := \begin{pmatrix} 1 & 0.33 & 0.11 & 1 \\ 3 & 1 & 0.33 & 3 \\ 9 & 3 & 1 & 9 \\ 1 & 0.33 & 0.11 & 1 \end{pmatrix} \quad A6 := \begin{pmatrix} 1 & 0.5 & 0.11 & 0.11 \\ 2 & 1 & 0.2 & 0.2 \\ 9 & 5 & 1 & 1 \\ 9 & 5 & 1 & 1 \end{pmatrix} \quad A7 := \begin{pmatrix} 1 & 0.5 & 0.14 & 1 \\ 2 & 1 & 0.25 & 2 \\ 7 & 4 & 1 & 7 \\ 1 & 0.5 & 0.14 & 1 \end{pmatrix} \quad A8 := \begin{pmatrix} 1 & 4 & 2 & 8 \\ 0.25 & 1 & 0.33 & 3 \\ 0.5 & 3 & 1 & 9 \\ 0.13 & 0.33 & 0.11 & 1 \end{pmatrix}$$

$$A9 := \begin{pmatrix} 1 & 0.5 & 0.33 & 0.33 \\ 2 & 1 & 0.5 & 0.5 \\ 3 & 2 & 1 & 1 \\ 3 & 2 & 1 & 1 \end{pmatrix} \quad A10 := \begin{pmatrix} 1 & 1 & 0.5 & 0.33 \\ 1 & 1 & 0.5 & 0.33 \\ 2 & 2 & 1 & 1 \\ 3 & 3 & 1 & 1 \end{pmatrix}$$

A1...A10 - матриці парних порівнянь топологій сучас СКМ за кожним показником

$$BB := \begin{pmatrix} 1 & 1 & 1 & 0.33 & 0.2 & 1 & 1 & 0.33 & 0.11 & 0.11 \\ 1 & 1 & 5 & 0.33 & 1 & 1 & 3 & 1 & 0.33 & 0.2 \\ 1 & 0.2 & 1 & 1 & 0.2 & 0.33 & 0.33 & 0.33 & 0.14 & 0.14 \\ 3 & 3 & 3 & 1 & 0.33 & 1 & 1 & 1 & 0.33 & 0.33 \\ 5 & 1 & 5 & 3 & 1 & 1 & 5 & 1 & 1 & 1 \\ 1 & 1 & 3 & 1 & 1 & 1 & 1 & 0.33 & 0.11 & 0.11 \\ 1 & 1 & 3 & 1 & 0.2 & 1 & 1 & 1 & 0.33 & 0.33 \\ 3 & 1 & 3 & 1 & 1 & 3 & 1 & 1 & 1 & 1 \\ 9 & 3 & 7 & 3 & 1 & 9 & 3 & 1 & 1 & 1 \\ 9 & 5 & 7 & 3 & 1 & 9 & 3 & 1 & 1 & 1 \end{pmatrix}$$

BB - матриця парних порівнянь показників для топологій СКМ

$i := 1..Ntm \qquad j := 1..Ntm$

$k := 1..Nttx \qquad n := 1..Nttx \qquad k1 := 1..Nttx - 1 \qquad n1 := 1..Nttx - 1$

Визначення власних значень кожної матриці A1...A10

$ev1 := ((eigenvals(A1))) \qquad ev2 := ((eigenvals(A2))) \qquad ev3 := ((eigenvals(A3)))$

$ev4 := ((eigenvals(A4))) \qquad ev5 := ((eigenvals(A5))) \qquad ev6 := ((eigenvals(A6)))$

$ev7 := ((eigenvals(A7))) \qquad ev8 := ((eigenvals(A8))) \qquad ev9 := ((eigenvals(A9)))$

$ev10 := ((eigenvals(A10)))$

Визначення власних значень матриці BB

$evBB := ((eigenvals(BB)))$

Визначення максимального власного значення кожної матриці A1...A10 та відповідного йому власно вектора

$Reav1 := Re(max(ev1)) \qquad Reav1 = 4.016 \qquad X1 := eigenvec(A1, Reav1)$

$Reav2 := Re(max(ev2)) \qquad Reav2 = 4.016 \qquad X2 := eigenvec(A2, Reav2)$

$Reav3 := Re(max(ev3)) \qquad Reav3 = 4.013 \qquad X3 := eigenvec(A3, Reav3)$

$Reav4 := Re(max(ev4)) \qquad Reav4 = 4.001 \qquad X4 := eigenvec(A4, Reav4)$

$Reav5 := Re(max(ev5)) \qquad Reav5 = 3.987 \qquad X5 := eigenvec(A5, Reav5)$

$Reav6 := Re(max(ev6)) \qquad Reav6 = 3.996 \qquad X6 := eigenvec(A6, Reav6)$

$Reav7 := Re(max(ev7)) \qquad Reav7 = 3.992 \qquad X7 := eigenvec(A7, Reav7)$

$Reav8 := Re(max(ev8)) \qquad Reav8 = 4.069 \qquad X8 := eigenvec(A8, Reav8)$

$Reav9 := Re(max(ev9)) \qquad Reav9 = 4.005 \qquad X9 := eigenvec(A9, Reav9)$

$Reav10 := Re(max(ev10)) \qquad Reav10 = 4.016 \qquad X10 := eigenvec(A10, Reav10)$

$$ev1 = \begin{pmatrix} 4.016 \\ -8.209 \times 10^{-3} + 0.275i \\ -8.209 \times 10^{-3} - 0.275i \\ 0 \end{pmatrix}$$

$$X1 = \begin{pmatrix} 0.789 \\ 0.44 \\ 0.422 \\ 0.073 \end{pmatrix} \quad X2 = \begin{pmatrix} 0.581 \\ 0.581 \\ 0.528 \\ 0.215 \end{pmatrix} \quad X3 = \begin{pmatrix} 0.671 \\ 0.637 \\ 0.353 \\ 0.136 \end{pmatrix} \quad X4 = \begin{pmatrix} 0.091 \\ 0.169 \\ 0.864 \\ 0.465 \end{pmatrix} \quad X5 = \begin{pmatrix} 0.104 \\ 0.312 \\ 0.939 \\ 0.104 \end{pmatrix}$$

$$X6 = \begin{pmatrix} 0.075 \\ 0.143 \\ 0.698 \\ 0.698 \end{pmatrix} \quad X7 = \begin{pmatrix} 0.13 \\ 0.254 \\ 0.95 \\ 0.13 \end{pmatrix} \quad X8 = \begin{pmatrix} 0.81 \\ 0.198 \\ 0.546 \\ 0.075 \end{pmatrix} \quad X9 = \begin{pmatrix} 0.2 \\ 0.349 \\ 0.647 \\ 0.647 \end{pmatrix} \quad X10 = \begin{pmatrix} 0.263 \\ 0.263 \\ 0.587 \\ 0.719 \end{pmatrix}$$

$LamA := (Reav1 \quad Reav2 \quad Reav3 \quad Reav4 \quad Reav5 \quad Reav6 \quad Reav7 \quad Reav8 \quad Reav9 \quad Reav10)$

$LamA =$

	1	2	3	4	5	6	7	8	9	10
1	4.016	4.016	4.013	4.001	3.987	3.996	3.992	4.069	4.005	4.016

Вектор власних значень матриць A1...A10

Визначення максимального власного значення матриці BB та відповідного йому власного вектора

$ReavBB := Re(max(evBB))$

$ReavBB = 11.359$

$XBB := eigenvec(BB, ReavBB)$ $XBB =$

	1
1	0.091
2	0.204
3	0.074
4	0.211
5	0.385
6	0.144
7	0.155
8	0.289
9	0.54
10	0.576

Власний вектор XBB - є вектором локальних пріоритетів показників, що використовуються під час порівняння топологій сучасних СКМ

Пошук індекса узгодженості для кожної із матриць A1...A10, а також матриці BB

$$IndSglA := \frac{LamA - Ntm}{(Ntm - 1)}$$

$$IndSglBB := \frac{ReavBB - Nttx}{(Nttx - 1)}$$

$IndSglA =$

	1	2	3	4	5	6	7	8
1	$472 \cdot 10^{-3}$	$367 \cdot 10^{-3}$	$447 \cdot 10^{-3}$	$075 \cdot 10^{-4}$	$176 \cdot 10^{-3}$	$251 \cdot 10^{-3}$	$713 \cdot 10^{-3}$	0.023

Пошук коефіцієнта відносної узгодженості для кожної із матриць A1...A10, а також матриці BB

$$OtnSgA := \left(\frac{IndSglA}{IsogA} \cdot 100\right) \qquad OtnSgBB := \left(\frac{IndSglBB}{IsogB} \cdot 100\right)$$

$OtnSgA =$

	1	2	3	4	5	6	7	8	9	10
1	0.608	0.596	0.494	0.023	0.464	0.139	0.301	2.571	0.184	0.596

$OtnSgBB = 10.131$

*Для кожної з матриць **A1...A10** та матриці **BB** коефіцієнти відносної узгодженості менше 10 %. Таки чином кожна матриця сформована правильно й може бути використаною для подальших розрахун*

Формування матриці AB із власних векторів матриць A1...A10

$Xy1 := augment(X1, X2)$ $Xy2 := augment(Xy1, X3)$ $Xy3 := augment(Xy2, X4)$ $Xy4 := augment(Xy3, X5)$

$Xy5 := augment(Xy4, X6)$ $Xy6 := augment(Xy5, X7)$ $Xy7 := augment(Xy6, X8)$ $Xy8 := augment(Xy7, X9)$

$AB := augment(Xy8, X10)$ $AB =$

	1	2	3	4	5	6	7	8	9	10
1	0.789	0.581	0.671	0.091	0.104	0.075	0.13	0.81	0.2	0.263
2	0.44	0.581	0.637	0.169	0.312	0.143	0.254	0.198	0.349	0.263
3	0.422	0.528	0.353	0.864	0.939	0.698	0.95	0.546	0.647	0.587
4	0.073	0.215	0.136	0.465	0.104	0.698	0.13	0.075	0.647	0.719

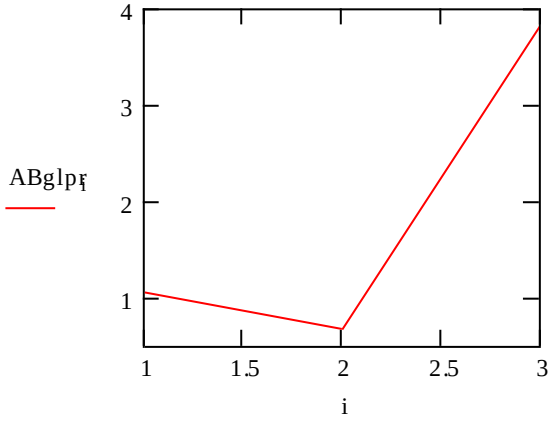
Нормування значень матриці AB (по стовпцям) до одиниці:

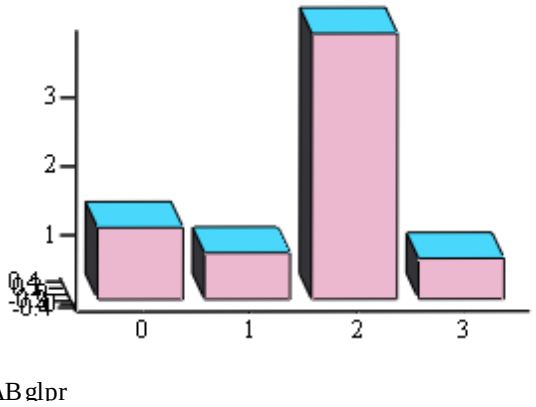
$$ABn_{i,k} := \frac{AB_{i,k}}{\sum_{i=1}^{Ntm} AB_{i,k}} \qquad ABn =$$

	1	2	3	4	5	6	7	8	9	10
1	0.458	0.305	0.373	0.057	0.071	0.047	0.089	0.497	0.109	0.144
2	0.255	0.305	0.355	0.107	0.214	0.089	0.173	0.122	0.189	0.144
3	0.245	0.277	0.196	0.544	0.644	0.432	0.649	0.335	0.351	0.321
4	0.042	0.113	0.076	0.292	0.071	0.432	0.089	0.046	0.351	0.392

Обчислення вектору гловальних пріоритетів, що дозволять визначити місце кожної з топологій сучасних СКМ, що порівнюються

$$ABglpr_i := \left[\sum_{kk=1}^{Nttx} \left(AB_{i,kk} - XBB_{kk} \right) \right] \qquad ABglpr = \begin{pmatrix} 1.046 \\ 0.678 \\ 3.864 \\ 0.592 \end{pmatrix}$$





Додаток В

Лістинг програми порівняльного оцінювання ПЗ однакового функціонального призначення за змішаними показниками

Порівняння СУБД за методом аналізу ієрархій

R1 - СУБД *Oracle Enterprise Edition*
R2 - СУБД *IBM DB2*
R3 - СУБД *Microsoft SQL Server*

ORIGIN:= 1

IsogD := 0.58 IsogKK1 := 0.58 IsogKK2 := 1.24 IsogKK3 := 0.58 IsogTTX := 1.49 IsogA := 1.49 IsogB := 1.5

F1 - фактор реалізації моделі даних
К1 - критерій підтримки об'єктно-орієнтованої моделі даних
К2 - критерій підтримки стандартних типів реляційних БД
F2 - фактор функціональних можливостей
К3 - критерій забезпечення оптимізації запитів
К4 - критерій забезпечення підтримки мережних протоколів
К5 - критерій забезпечення розподіленої обробки даних
К6 - критерій забезпечення зберігання /обробки/ мультимедіа та геопросторових даних
К7 - критерій забезпечення багатомірного аналізу інформації
F3 - фактор надійності
К8 - критерій можливості відновлення після збоїв
К9 - критерій можливості резервного копіювання та відновлення змін
К10- критерій можливості захисту від несанкціонованого доступу

І. Визачення функції, застосування якої є визначальною при виборі СУБД

1.1 Формування матриці парного порівняння функцій F1...F3

NFakt := 3 - кількість факторів $D1 := \begin{pmatrix} 1 & 0.25 & 0.33 \\ 4 & 1 & 2 \\ 3 & 0.5 & 1 \end{pmatrix}$

1.2 Визначення власних значень матриці D1: ev1 := ((eigenvals (D1))) $ev1 = \begin{pmatrix} 3.015 \\ -7.69\times 10^{-3} + 0.237i \\ -7.69\times 10^{-3} - 0.237i \end{pmatrix}$

1.3 Визначення максимального власного значення матриці D1 та відповідного йому власного вект

Reav1 := Re(max(ev1)) Reav1 = 3.015 d1 := eigenvec (D1, Reav1) $d1 = \begin{pmatrix} 0.186 \\ 0.853 \\ 0.488 \end{pmatrix}$

1.4 Пошук індекса узгодженості для матриці D1: $IndSglD1 := \frac{Reav1 - NFakt}{(NFakt - 1)}$ $IndSglD1 = 7.69\times 10^{-3}$

1.5 Пошук коефіцієнту відносної узгодженості для матриці D1 (якщо він менше 10 %то відповідно матриця сформована правильно та її можливо використовувати для подальших розрахунків) $OtnSgD1 := \left(\frac{IndSglD1}{IsogD}\cdot 100\right)$ OtnSgD1 = 1.326

1.6 Нормуємо власні значення матриці D1 до одиниці: i := 1.. NFakt $d1n_i := \frac{d1_i}{\sum_{i=1}^{NFakt} d1_i}$ $d1n = \begin{pmatrix} 0.122 \\ 0.559 \\ 0.32 \end{pmatrix}$

ВИСНОВОК: ***Найбільш визачальними при виборі СУБД є функції функціональних можливостей (F2) та надійності(F3)***

II. Визначення критеріїв, які є визначальними у кожній із функцій

2.1 Формування матриць парних порівнянь критеріїв K1...K2 за функцією F1, критеріїв K3...K7 за функцією F2, критеріїв K8...K10 за функцією F3.

$NFakt1 := 2$ - кількість критеріїв за функцією F1

$NFakt2 := 5$ - кількість критеріїв за функцією F2

$NFakt3 := 3$ - кількість критеріїв за функцією F3

$$KK1 := \begin{pmatrix} 1 & 4 \\ 0.25 & 1 \end{pmatrix} \quad KK2 := \begin{pmatrix} 1 & 0.14 & 0.25 & 0.5 & 0.33 \\ 7 & 1 & 3 & 5 & 4 \\ 4 & 0.33 & 1 & 4 & 3 \\ 2 & 0.2 & 0.25 & 1 & 0.5 \\ 3 & 0.25 & 0.33 & 2 & 1 \end{pmatrix} \quad KK3 := \begin{pmatrix} 1 & 3 & 2 \\ 0.33 & 1 & 0.25 \\ 0.5 & 4 & 1 \end{pmatrix}$$

2.2 Визначення власних значень матриць KK1, KK2 та KK3:

$evKK1 := ((eigenvals(KK1)))$ $evKK2 := ((eigenvals(KK2)))$ $evKK3 := ((eigenvals(KK3)))$

$$evKK1 = \begin{pmatrix} 2 \\ 0 \end{pmatrix} \quad evKK2 = \begin{pmatrix} 5.142 \\ -5.311 \times 10^{-3} + 0.879i \\ -5.311 \times 10^{-3} - 0.879i \\ -0.066 + 0.02i \\ -0.066 - 0.02i \end{pmatrix} \quad evKK3 = \begin{pmatrix} 3.103 \\ -0.052 + 0.572i \\ -0.052 - 0.572i \end{pmatrix}$$

2.3 Визначення максимальних власних значень матриць KK1, KK2, KK3 та відповідних ним власних векторів

$ReavKK1 := Re(max(evKK1))$ $ReavKK1 = 2$ $Xkk1 := eigenvec(KK1, ReavKK1)$ $Xkk1 = \begin{pmatrix} 0.97 \\ 0.243 \end{pmatrix}$

$ReavKK2 := Re(max(evKK2))$ $ReavKK2 = 5.142$ $Xkk2 := eigenvec(KK2, ReavKK2)$ $Xkk2 = \begin{pmatrix} 0.09 \\ 0.852 \\ 0.446 \\ 0.138 \\ 0.219 \end{pmatrix}$

$ReavKK3 := Re(max(evKK3))$ $ReavKK3 = 3.103$ $Xkk3 := eigenvec(KK3, ReavKK3)$ $Xkk3 = \begin{pmatrix} 0.807 \\ 0.193 \\ 0.559 \end{pmatrix}$

2.4 Пошук індексів узгодженості для матриць KK1, KK2 та KK3:

$$IndSglKK1 := \frac{ReavKK1 - NFakt1}{(NFakt1 - 1)} \qquad IndSglKK1 = 0$$

$$IndSglKK2 := \frac{ReavKK2 - NFakt2}{(NFakt2 - 1)} \qquad IndSglKK2 = 0.035$$

$$IndSglKK3 := \frac{ReavKK3 - NFakt3}{(NFakt3 - 1)} \qquad IndSglKK3 = 0.052$$

2.5 Пошук коефіцієнту відносної узгодженості для матриць KK1, KK2 та KK3 (якщо вони менше, ніж 10 % відповідно матриці сформовані правильно та їх можна використовувати для подальших розрахунків)

$$OtnSgKK1 := \left(\frac{IndSglKK1}{IsogKK1} \cdot 100\right) \qquad OtnSgKK2 := \left(\frac{IndSglKK2}{IsogKK2} \cdot 100\right) \qquad OtnSgKK3 := \left(\frac{IndSglKK3}{IsogKK3} \cdot 100\right)$$

$OtnSgKK1 = 0$ $OtnSgKK2 = 2.858$ $OtnSgKK3 = 8.898$

2.6 Нормування власних значеннь матриць KK1, KK2 та KK3 до одиниці:

$i := 1..NFakt1$ $l := 1..NFakt2$ $j := 1..NFakt3$

$$Xkk1n_i := \frac{Xkk1_i}{\sum_{i=1}^{NFakt1} Xkk1_i} \qquad Xkk2n_l := \frac{Xkk2_l}{\sum_{l=1}^{NFakt2} Xkk2_l} \qquad Xkk3n_j := \frac{Xkk3_j}{\sum_{j=1}^{NFakt3} Xkk3_j}$$

$$Xkk1n = \begin{pmatrix} 0.8 \\ 0.2 \end{pmatrix} \qquad Xkk2n = \begin{pmatrix} 0.051 \\ 0.489 \\ 0.256 \\ 0.079 \\ 0.125 \end{pmatrix} \qquad Xkk3n = \begin{pmatrix} 0.518 \\ 0.124 \\ 0.359 \end{pmatrix}$$

ВИСНОВОК: ***Найбільш визачальними за функцією F1 є критерій К1;***
за функцією F2 є критерії К4 та К5;
за функцією F3 є критерії К8 та К10.

III. Визачення локальних пріоритетів критеріїв якості (ТТХ) порівнюваних СУБД

3.1 Формування матриці парних порівнянь усіх критеріїв К1...К10 між собою

$$TTX := \begin{pmatrix} 1 & 2 & 5 & 3 & 0.33 & 0.25 & 3 & 2 & 0.5 & 0.33 \\ 0.5 & 1 & 3 & 2 & 4 & 3 & 2 & 0.5 & 0.33 & 0.25 \\ 0.2 & 0.33 & 1 & 0.5 & 0.25 & 0.33 & 0.2 & 0.16 & 0.14 & 0.25 \\ 0.33 & 0.5 & 2 & 1 & 3 & 5 & 4 & 0.25 & 0.33 & 0.25 \\ 3 & 0.25 & 4 & 0.33 & 1 & 3 & 5 & 0.5 & 0.2 & 0.33 \\ 4 & 0.33 & 3 & 0.2 & 0.33 & 1 & 3 & 0.33 & 0.5 & 0.25 \\ 0.33 & 0.5 & 5 & 0.25 & 0.2 & 0.33 & 1 & 0.16 & 0.2 & 0.14 \\ 0.5 & 2 & 6 & 4 & 2 & 3 & 6 & 1 & 3 & 2 \\ 2 & 3 & 7 & 3 & 5 & 2 & 5 & 0.33 & 1 & 0.14 \\ 3 & 4 & 4 & 4 & 3 & 4 & 7 & 2 & 7 & 1 \end{pmatrix}$$

$NCYBD := 3$ - кількість СУБД

$NTTX := 10$ - кількість ТТХ

3.2 Визначення власних значень матриці ТТХ, її максимального власного значення та відповідного йому власного вектора

$evTTX := ((eigenvals(TTX)))$

$ReavTTX := Re(max(evTTX))$ $\quad ReavTTX = 12.914$

$ttx := eigenvec(TTX, ReavTTX)$

$evTTX =$

	1
1	12.914
2	-0.455+4.427i
3	-0.455-4.427i
4	-0.072+3.224i
5	-0.072-3.224i
6	0.056+1.505i
7	0.056-1.505i
8	-1.501
9	0.19
10	-0.662

$ttx =$

	1
1	.249
2	.226
3	.053
4	.207
5	.207
6	.172
7	.071
8	.457
9	.348
10	.659

3.3 Пошук індекса узгодженості для матриці ТТХ:

$$IndSglTTX := \frac{ReavTTX - NTTX}{(NTTX - 1)} \qquad IndSglTTX = 0.324$$

3.4 Пошук коефіцієнту відносної узгодженості для матриці ТТХ (якщо він менше 10 %, то відповідно матриця сформована правильно та її можливо використовувати для подальших розрахунків)

$$OtnSgTTX := \left(\frac{IndSglTTX}{IsogTTX} \cdot 100 \right) \qquad OtnSgTTX = 21.733 \qquad i := 1..NTTX$$

3.5 Нормування власних значень матриці ТТХ до одиниці та отримання набору локальних пріоритетів ТТХ:

$$ttxn_i := \frac{ttx_i}{\sum_{i=1}^{NTTX} ttx_i}$$

$ttxn =$

	1
1	0.094
2	0.085
3	0.02
4	0.078
5	0.078
6	0.065
7	0.027
8	0.172
9	0.131
10	0.249

$$ttx1 := \sum_{i=1}^{NTTX} ttx_i \qquad ttx1 = 2.649 \qquad ttxn1 := \sum_{i=1}^{NTTX} ttxn_i \qquad ttxn1 = 1$$

3.6 Формування матриці балів кожної ТТХ для порівнюваних СУБД - "B", наданих, наприклад, 3 експер та вектора-стовпця вагових коефіцієнтів важливості кожної з них

$$B := \begin{pmatrix} 3 & 4 & 4 \\ 3 & 3 & 3 \\ 3 & 2 & 4 \\ 4 & 3 & 3 \\ 3 & 5 & 4 \\ 3 & 3 & 2 \\ 2 & 3 & 2 \\ 4 & 3 & 4 \\ 3 & 4 & 3 \\ 4 & 4 & 3 \end{pmatrix}$$

$Nekc := 3$ Кількість експертів

$NTTX := 10$ Кількість експертів

$h := 1..Nekc \qquad k := 1..NTTX$

Обчислення у балах і нормування ваги кожної ТТХ, що надана кожним експертом ($Bb_{k,h}$) та обчислення середнього значення вагового коефіцієнта кожної ТТХ (bn_k):

$$Bb_{k,h} := \frac{B_{k,h}}{\sum_{k=1}^{NTTX} B_{k,h}} \qquad bn_k := \frac{\sum_{h=1}^{Nekc} Bb_{k,h}}{\sum_{h=1}^{Nekc}\sum_{k=1}^{NTTX} Bb_{k,h}}$$

$Bb =$

	1	2	3
1	0.094	0.118	0.125
2	0.094	0.088	0.094
3	0.094	0.059	0.125
4	0.125	0.088	0.094
5	0.094	0.147	0.125
6	0.094	0.088	0.063
7	0.063	0.088	0.063
8	0.125	0.088	0.125
9	0.094	0.118	0.094
10	0.125	0.118	0.094

$bn =$

	1
1	0.112
2	0.092
3	0.093
4	0.102
5	0.122
6	0.081
7	0.071
8	0.113
9	0.102
10	0.112

$$bcym := \sum_{k=1}^{NTTX} bn_k \qquad bcym = 1$$

ВИСНОВОК:

1. Найбільш визачальними критеріями, що впливають на вибір СУБД є критерії К1, К4, К5, К8 та К10.

2. З урахуванням міркувань експертів перелік визначальних критеріїв залишається таким же незмінним, а саме: К1, К4, К5, К8 та К10.

IV. Визачення раціональної СУБД за сукупністю критеріїв якості

4.1 Формування матриці парних порівнянь СУБД за кожною ТТХ:

$$A1 := \begin{pmatrix} 1 & 4 & 3 \\ 0.25 & 1 & 2 \\ 0.33 & 0.5 & 1 \end{pmatrix} \quad A2 := \begin{pmatrix} 1 & 0.5 & 0.16 \\ 2 & 1 & 0.33 \\ 7 & 3 & 1 \end{pmatrix} \quad A3 := \begin{pmatrix} 1 & 0.14 & 0.16 \\ 6 & 1 & 0.5 \\ 7 & 2 & 1 \end{pmatrix} \quad A4 := \begin{pmatrix} 1 & 3 & 4 \\ 0.33 & 1 & 2 \\ 0.25 & 0.5 & 1 \end{pmatrix} \quad A5 := \begin{pmatrix} 1 & 0.25 & 0.33 \\ 4 & 1 & 5 \\ 3 & 0.2 & 1 \end{pmatrix}$$

$$A6 := \begin{pmatrix} 1 & 5 & 2 \\ 0.2 & 1 & 0.25 \\ 0.5 & 4 & 1 \end{pmatrix} \quad A7 := \begin{pmatrix} 1 & 0.14 & 0.25 \\ 7 & 1 & 1 \\ 4 & 1 & 1 \end{pmatrix} \quad A8 := \begin{pmatrix} 1 & 2 & 5 \\ 0.5 & 1 & 5 \\ 0.2 & 0.2 & 1 \end{pmatrix} \quad A9 := \begin{pmatrix} 1 & 3 & 2 \\ 0.33 & 1 & 2 \\ 0.5 & 0.5 & 1 \end{pmatrix} \quad A10 := \begin{pmatrix} 1 & 0.33 & 0.25 \\ 3 & 1 & 2 \\ 4 & 0.5 & 1 \end{pmatrix}$$

4.2 Визначення власних значень матриць A1, A2, A3, A4, A5, A6, A7, A8, A9 та A10:

$ev1 := ((eigenvals(A1)))$ $ev2 := ((eigenvals(A2)))$ $ev3 := ((eigenvals(A3)))$ $ev4 := ((eigenvals(A4)))$

$ev5 := ((eigenvals(A5)))$ $ev6 := ((eigenvals(A6)))$ $ev7 := ((eigenvals(A7)))$ $ev8 := ((eigenvals(A8)))$

$ev9 := ((eigenvals(A9)))$ $ev10 := ((eigenvals(A10)))$

4.3 Визначення максимальних власних значень матриць A1...A12 та відповідних ним власних векторів

$Reav1 := Re(max(ev1))$ $Reav1 = 3.103$ $X1 := eigenvec(A1, Reav1)$

$Reav2 := Re(max(ev2))$ $Reav2 = 3.037$ $X2 := eigenvec(A2, Reav2)$

$Reav3 := Re(max(ev3))$ $Reav3 = 3.036$ $X3 := eigenvec(A3, Reav3)$

$Reav4 := Re(max(ev4))$ $Reav4 = 3.015$ $X4 := eigenvec(A4, Reav4)$

$Reav5 := Re(max(ev5))$ $Reav5 = 3.195$ $X5 := eigenvec(A5, Reav5)$

$$ev6 = \begin{pmatrix} 3.025 \\ -0.012 + 0.272i \\ -0.012 - 0.272i \end{pmatrix}$$

$Reav6 := Re(max(ev6))$ $Reav6 = 3.025$ $X6 := eigenvec(A6, Reav6)$

$Reav7 := Re(max(ev7))$ $Reav7 = 3.029$ $X7 := eigenvec(A7, Reav7)$

$Reav8 := Re(max(ev8))$ $Reav8 = 3.054$ $X8 := eigenvec(A8, Reav8)$

$Reav9 := Re(max(ev9))$ $Reav9 = 3.133$ $X9 := eigenvec(A9, Reav9)$

$Reav10 := Re(max(ev10))$ $Reav10 = 3.103$ $X10 := eigenvec(A10, Reav10)$

$$X1 = \begin{pmatrix} 0.922 \\ 0.319 \\ 0.221 \end{pmatrix} \quad X2 = \begin{pmatrix} 0.147 \\ 0.297 \\ 0.943 \end{pmatrix} \quad X3 = \begin{pmatrix} 0.102 \\ 0.511 \\ 0.854 \end{pmatrix} \quad X4 = \begin{pmatrix} 0.916 \\ 0.348 \\ 0.2 \end{pmatrix} \quad X5 = \begin{pmatrix} 0.152 \\ 0.944 \\ 0.293 \end{pmatrix}$$

$$X6 = \begin{pmatrix} 0.854 \\ 0.146 \\ 0.499 \end{pmatrix} \quad X7 = \begin{pmatrix} 0.131 \\ 0.763 \\ 0.633 \end{pmatrix} \quad X8 = \begin{pmatrix} 0.839 \\ 0.528 \\ 0.133 \end{pmatrix} \quad X9 = \begin{pmatrix} 0.86 \\ 0.413 \\ 0.298 \end{pmatrix} \quad X10 = \begin{pmatrix} 0.193 \\ 0.807 \\ 0.559 \end{pmatrix}$$

4.4 Формування вектора власних значень матриць A1...A10

$LamA := (Reav1 \ \ Reav2 \ \ Reav3 \ \ Reav4 \ \ Reav5 \ \ Reav6 \ \ Reav7 \ \ Reav8 \ \ Reav9 \ \ Reav10)$

$LamA =$

	1	2	3	4	5	6	7	8	9	10
1	3.103	3.037	3.036	3.015	3.195	3.025	3.029	3.054	3.133	3.103

4.5 Пошук індексів узгодженості для матриць A1...A10:

$$IndSglA := \frac{LamA - NCYBD}{(NCYBD - 1)}$$

$IndSglA =$

	1	2	3	4	5	6	7	8
1	0.052	0.018	0.018	$1.69 \cdot 10^{-3}$	0.098	0.012	0.015	0.027

4.6 Пошук коефіцієнтів відносної узгодженості для матриць A1...A10 (якщо вони менше 20 %, то відповідно матриці сформовані правильно та їх можливо використовувати для подальших розрахунків

$$OtnSgA := \left(\frac{IndSglA}{IsogA} \cdot 100 \right) \qquad OtnSgA =$$

	1	2	3	4	5	6	7	8	9	10
1	3.464	1.234	1.196	0.516	6.548	0.825	0.985	1.799	4.473	3.464

4.7 Формування матриці AB із власних векторів матриць A1...A10:

$Xy1 := augment(X1, X2)$ $Xy2 := augment(Xy1, X3)$ $Xy3 := augment(Xy2, X4)$ $Xy4 := augment(Xy3, X5)$

$Xy5 := augment(Xy4, X6)$ $Xy6 := augment(Xy5, X7)$ $Xy7 := augment(Xy6, X8)$ $Xy8 := augment(Xy7, X9)$

$AB := augment(Xy8, X10)$ $AB =$

	1	2	3	4	5	6	7	8	9	10
1	0.922	0.147	0.102	0.916	0.152	0.854	0.131	0.839	0.86	0.193
2	0.319	0.297	0.511	0.348	0.944	0.146	0.763	0.528	0.413	0.807
3	0.221	0.943	0.854	0.2	0.293	0.499	0.633	0.133	0.298	0.559

4.8 Нормування власних значень матриць A1...A10 до одиниці: $i := 1..NCYBD$ $k := 1..NTTX$

$$ABn_{i,k} := \frac{AB_{i,k}}{\sum_{i=1}^{NCYBD} AB_{i,k}} \qquad Sym1 := \sum_{i=1}^{NCYBD} AB_{i,1} \qquad Sym11n := \frac{AB_{1,1}}{Sym1} \qquad ABn1_k := \sum_{i=1}^{NCYBD} ABn_{i,k}$$

$Sym1 = 1.461$ $Sym11n = 0.631$

$ABn =$

	1	2	3	4	5	6	7	8	9	10
1	0.631	0.106	0.07	0.625	0.109	0.57	0.086	0.559	0.547	0.124
2	0.218	0.214	0.348	0.238	0.68	0.097	0.5	0.352	0.263	0.518
3	0.151	0.68	0.582	0.137	0.211	0.333	0.415	0.089	0.19	0.359

$ABn1 =$

2	1
3	1
4	1
5	1
6	1
7	1
8	1
9	1
10	1

$$i := 1..NCYBD \qquad CYBD1_i := \left(\sum_{k=1}^{NTTX} ABn_{i,k} \cdot ttxn_k \right) \cdot 100 \qquad CYBD1 = \begin{pmatrix} 36.541 \\ 36.133 \\ 27.325 \end{pmatrix}$$

$$CYBD1n_i := \frac{CYBD1_i}{\min(CYBD1)} \qquad CYBD1n = \begin{pmatrix} 1.337 \\ 1.322 \\ 1 \end{pmatrix}$$

*4.9 Формування набору **глобальних пріоритетів порівнюваних СУБД** з урахуванням міркувань, наприклад, 3-х експертів та вираження результату у %:*

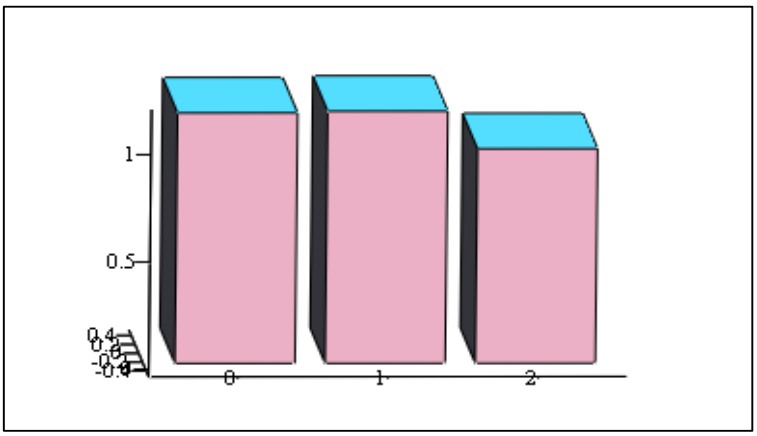
$$i := 1..NCYBD \qquad CYBDzag_i := \left(\sum_{k=1}^{NTTX} ABn_{i,k} \cdot bn_k \right) \cdot 100 \qquad CYBDzag = \begin{pmatrix} 34.931 \\ 35.157 \\ 29.912 \end{pmatrix}$$

$$CYBDnzag_i := \frac{CYBDzag_i}{\min(CYBDzag)} \qquad CYBDnzag = \begin{pmatrix} 1.168 \\ 1.175 \\ 1 \end{pmatrix}$$

Враховуючи, що СУБД *Microsoft SQL Server* має мінімальний пріоритет, оберемо її в якості базового зразка при розрахунку узагальненого показника якості для решти СУБД із сукупності досліджуваних. Виходячи з цього загальний результат матиме вид:

ВИСНОВОК:

Найбільш функціональним та надійним, як видно з результату, є: СУБД *IBM DB2.*



CYBDnzag

Додаток Г

Лістинг програми кластеризації об’єктів для вирішення задачі детектування і відновлення даних

```
{                  ПРОГРАМА ВИКОРИСТАННЯ  ПРИНЦИПУ САМООРГАНІЗАЦІЇ                  }
{------------------------------------ ПРИ НЕЧІТКІЙ КЛАСТЕРИЗАЦІЇ-----------------------------------}
{     З нормуванням за максимальним значенням та урахуванням тільки кількісних при знаків   }
{     Проводиться розрахунок коеф. несуперечності по двом деревам з процедурою              }
{     регуляризації повного перебору і виведенням коеф.непр.                                }
{------------------------------------ введення вихідних даних ----------------------------------------}
USES CRT,MATR3F5,Stop_REZ{,WinAPI};
const
  {n=6;{кількість об'єктів}
  {p=2;{кількість кількісних ознак}
  kl=2; {кількість якісних ознак     }
  n4=7;{потужність неч. множини 4-ї ознаки}
  n5=4;{потужність неч. множини 5-ї ознаки}
var
  f1,f2,f3:text;  {f1-файл відсічених диполей}
             {f2,f3-файли дерев}
  p4,p5:tp4;
  a,a1,sora,sorb,sora1,sorb1,cy1:te5;
  z1,b1,zA,zB: varte6;
  e4,e5,e,m1,m:varte7;
  pa,pb:varte7;
  bA,bB,bA1,bB1:varte8;
  i,j,i1,i2,i3,i4{,kd1,k11},r:integer;
  iz,jz:integer;{змінні для дорегуляризації}
  r1:integer; {змінна для організації циклу для довизначення}
  ps1,ps2,ps3,ost,ost1,ost2:real;
  {p4:array[1..n,1..n4] of real;}{масив якіс. приз.4-ї ознаки}
  {p5:array[1..n,1..n5] of real;}{масив якіс. приз.5-ї ознаки}
  ps:array[1..p] of real;{масив серед.значень}
  j11:integer;
  z:array [1..100] of integer;
BEGIN
ClrScr;
 {writeln ('Введіть число об'єктів n=');
 readln (n);
 writeln ('Введіть число кількісних ознак p=');
 readln (p);}
    {------------якісні  ознаки--------------------}
 {низький-S1}    { низький -S2}  {серед.-S3}    {серед-S4}     { низький -S5}
 {p4[1,1]:=0.7; p4[2,1]:=0.7; p4[3,1]:=0.2; p4[4,1]:=0.2; p4[5,1]:=0.7;
 p4[1,2]:=0.2; p4[2,2]:=0.2; p4[3,2]:=0;   p4[4,2]:=0;   p4[5,2]:=0.2;
 p4[1,3]:=0;   p4[2,3]:=0;   p4[3,3]:=0;   p4[4,3]:=0;   p4[5,3]:=0;
 p4[1,4]:=0.6; p4[2,4]:=0.6; p4[3,4]:=0.6; p4[4,4]:=0.6; p4[5,4]:=0.6;
 p4[1,5]:=0.5; p4[2,5]:=0.5; p4[3,5]:=0.8; p4[4,5]:=0.8; p4[5,5]:=0.5;
 p4[1,6]:=1;   p4[2,6]:=1;   p4[3,6]:=0.4; p4[4,6]:=0.4; p4[5,6]:=1;
 p4[1,7]:=0;   p4[2,7]:=0;   p4[3,7]:=1;   p4[4,7]:=1;   p4[5,7]:=0;}
  {серед.-S1}   {висок.-S2}   {серед.-S3}    { низький.-S4}    { низький.-S4}
  {p5[1,1]:=0;   p5[2,1]:=0.3; p5[3,1]:=0;   p5[4,1]:=1;   p5[5,1]:=1;
  p5[1,2]:=0.3; p5[2,2]:=1;   p5[3,2]:=0.3; p5[4,2]:=0.5; p5[5,2]:=0.5;
  p5[1,3]:=0.7; p5[2,3]:=0.5; p5[3,3]:=0.7; p5[4,3]:=0.5; p5[5,3]:=0.5;
  p5[1,4]:=1;   p5[2,4]:=0.8; p5[3,4]:=1;   p5[4,4]:=0.2; p5[5,4]:=0.2;}
   {------БЛОК вводу кількісних ознак ----------------------}
```

```
 for i:=1 to p do
   begin
     for j:=1 to n do
      begin
       writeln ('p1[',i,',',j,']='); readln (p1[i,j]);
      end;
   end;
  {p1[1,1]:=4;     p1[2,1]:=8.5;
  p1[1,2]:=12.5;  p1[2,2]:=4;
  p1[1,3]:=4;     p1[2,3]:=6;
  p1[1,4]:=7.5;   p1[2,4]:=2.5;
  p1[1,5]:=6;     p1[2,5]:=8.5 ;
  p1[1,6]:=11;    p1[2,6]:=5.5;
  p1[1,7]:=4.5;   p1[2,7]:=7.5;
  p1[1,8]:=2;     p1[2,8]:=11;
  p1[1,9]:=2;     p1[2,9]:=2;
  p1[1,10]:=7;    p1[2,10]:=7;
  p1[1,11]:=11;   p1[2,11]:=13;
  p1[1,12]:=7;    p1[2,12]:=14;
  p1[1,13]:=14;   p1[2,13]:=1;
  {p1[1,14]:=2;    p1[2,14]:=15;
  p1[1,15]:=13;   p1[2,15]:=10 ;
  p1[1,16]:=12;   p1[2,16]:=10;
  p1[1,17]:=12;   p1[2,17]:=9;
  p1[1,18]:=13;   p1[2,18]:=9;
  {p1[1,19]:=13;   p1[2,19]:=15;}
writeln (MemAvail, ' Байт вільно на початку програми');
readln;
{-----БЛОК 1.Нормування кількісних ознак ------------------}
{-------1.обчислення максимального значення----------------}
 Max_STR;
 {-------2.Нормування змінних----------------------}
{  writeln('НОРМОВАНІ КІЛЬКІСНІ ОЗНАКИ');}
 for i:=1 to p do
   begin
     for j:=1 to n do
      p1[i,j]:=p1[i,j]/max[i];
   end;
 {for i:=1 to p do
   begin
     for j:=1 to n do
      begin
      writeln(' p1^[',i,',',j,']=',p1[i,j]:4:4);
      end;
      readln;
   end;}
 {-----БЛОК 2.Блок отримання матриці близькості D ---------}
 {------1.обчислення евклідової відстані для кількісних змінних}
{writeln('    Сума евклідових відстаней за кількісними ознаками L[i,j]');}
{GETMEM (l, SizeOf(te7));}
 Ev_r;
 { for i:=1 to n  do
```

```
    begin
     for j:=1 to n  do
      begin
     write ('  l^[',i,',',j,']=',l[i]^[j]:4:4);
      end;
      readln;
    end;
  {------2. обчислення евклідової відстані для якісних змінних---}
 {writeln('    Сума евклідових відстаней за якісними ознаками e4[i,j]');}
{GETMEM (e4, SizeOf(te7));}
 Ev_r1 (n4,p4,e4);{процедура обчислення віднос. евкл.відст.повної}
  { for i:=1 to n  do
    begin
     for j:=1 to n  do
      begin
      write (' e4^[',i,',',j,']=',e4[i]^[j]:4:4);
      end;
      readln;
    end;
 {writeln('    Сума евклідових відстаней за якісними ознаками e5[i,j]');}
{GETMEM (e5, SizeOf(te7));}
 Ev_r1 (n5,p5,e5);{ процедура обчислення віднос. евкл.відст.повної}
   {for i:=1 to n  do
    begin
     for j:=1 to n  do
      begin
      write (' e5^[',i,',',j,']=',e5[i]^[j]:4:4);
      end;
      readln;
    end;
 {writeln('    Сума евклідових відстаней за якісними ознаками e[i,j]');}
{GETMEM (e, SizeOf(te7));}
 SUMMA (e4,e5,e);{процедура додавання e4 и e5}
  {for i:=1 to n  do
    begin
     for j:=1 to n  do
      begin
      write (' e^[',i,',',j,']=',e[i]^[j]:4:4);
      end;
      readln;
    end;
 writeln('    Сума всіх евклідових відстаней m1=l[i,j]+e[i,j]');}
{GETMEM (m1, SizeOf(te7));}
 SUMMA (l,e,m1);{процедура додавання l[i,j] и e[i,j]}
  {for i:=1 to n  do
    begin
     for j:=1 to n  do
      begin
      write (' m1[',i,',',j,']=',m1[i]^[j]:4:4);
      end;
      readln;
    end;}
```

```
{ writeln('    МАТРИЦЯ БЛИЗЬКОСТІ МАЄ ВИД                    ');}
{GETMEM (m, SizeOf(te7));}
 D_m (m1,m);{процедура надхождення матриці міжточкових відстаней}
  {for i:=1 to n  do
     begin
      for j:=1 to n  do
       begin
       write ('  m^[',i,',',j,']=',m[i]^[j]:4:4);
       end;
       readln;
     end;}
{очистка динамічної пам’яті}
  for i:=1 to n do
  begin
   FREEMEM (l[i], n*sizeof(real){SizeOf(te7)});
   FREEMEM (e4[i], n*sizeof(real){SizeOf(te7)});
   FREEMEM (e5[i], n*sizeof(real){SizeOf(te7)});
   FREEMEM (e[i], n*sizeof(real){SizeOf(te7)});
   FREEMEM (m1[i], n*sizeof(real){SizeOf(te7)});
  end;
writeln (MemAvail, ' Байт вільно після очистки l,e4,e5,e,m1 ');
readln;
Sor_1 (m,a); {процедура сортування елементів трикутної матриці}
 {---------ВИВЕДЕННЯ РЕЗУЛЬТАТІВ-------------------}
{writeln ('РЕЗУЛЬТАТ СОРТУВАННЯ');}
kd1:=(n*n-n) div 2;
    {for i:=1 to sz do
     {begin
      Stop_Kadr (i);
      writeln (' a[',i,']=',a[i]:4:4);
     end;
      readln;}
GETMEM (z1, SizeOf(te6));
Dip (a,m,z1); {    процедура формування диполів          }
{--------- ВИВЕДЕННЯ РЕЗУЛЬТАТІВ --------------------}
{writeln (' формування диполей за матрицею близькості');
for j:=1 to kd1 do
      begin
       Stop_Kadr1 (j);
       writeln ('Адрес диполя =',j,'--------------');
      write ('-z1[1,',j,']=',z1^[1,j],'   ');
      write ('-z1[2,',j,']=',z1^[2,j],'   ');
      writeln ('----a[',j,']=',a[j]:4:4);
      end;
      readln;}
GETMEM (b1, SizeOf(te6));
Dip1 (z1,b1);
{Процедура відсікання зайвих диполів для формування множин}
{--------- ВИВЕДЕННЯ РЕЗУЛЬТАТІВ -------------------------------}
{ writeln ('Диполі для формування підмножин');}
 ASSIGN (f1,'d:\Work_pr\Klast1f5\dipol4');
 REWRITE (f1);
```

```
      {for i:=1 to 2 do  begin
        for j:=1 to k1 do
          write ('  ',b1^[i,j]);
          writeln;
       end;
          readln;}
       for i:=1 to 2 do
        begin
         for j:=1 to k1 do
           begin
           write (f1,'  ',b1^[i,j]);
           end;
           {writeln;}
        end;
 FREEMEM (b1, SizeOf(te6));
 FREEMEM (z1, SizeOf(te6));
 {CLOSE (f1);}
 ASSIGN (f2,'d:\Work_pr\Klast1f5\PodA');
 ASSIGN (f3,'d:\Work_pr\Klast1f5\PodB');
{--- організація циклу для довизначення несуперечливих кластеризації --}
{----k1-- кількість диполів у відсіченій матриці диполів }
r1:=round(exp(k1*ln(2)));
 j11:=0;
  ost1:=0; iz:=0;
  REPEAT
  {for iz:=1 to 1{r1} {do}
   {Begin  {Початок  циклу  довизначення}
   iz:=iz+1;
   {зчитування з файлу}
    RESET(f1);
    for i:=1 to 2 do  begin
        for j:=1 to k1 do
          read (f1,b1^[i,j]);
          {writeln;}
      end;
   j11:=j11+1;
   for jz:=1 to k1 do
    begin
     if jz=1 then
      begin
       if odd(j11)=TRUE then z[jz]:=1 else z[jz]:=0
      end else
          begin
          i4:=round(int(j11/2));
          if odd(i4)=True then z[jz]:=1 else z[jz]:=0;
          j11:=i4;
          if jz=k1 then j11:=iz;
          end;
    end;
          {for i1:=1 to k1 do
          begin
           write (' ',z[i1]);
```

```
            write;
           end;
            readln;}
            {переворот диполей}
             for i1:=1 to k1 do
              begin
               if z[i1]<>0 then
                begin
                 i3:=b1^[1,i1];
                 b1^[1,i1]:=b1^[2,i1];
                 b1^[2,i1]:=i3;
                end;
               end;
              {----------------}
               {writeln ('Диполі для формування підмножин');}
               {for i:=1 to 2 do
               begin
                for j:=1 to k1 do
                 write ('  ',b1^[i,j]);
                 writeln;
               end;
                 readln;}
{-----------------------------------------------------------------}
Podmn (m,b1,pa,pb);
{ процедура формування підмножин по діполям та }
{матриці близькості---------------------------------------}
{--------- ВИВЕДЕННЯ РЕЗУЛЬТАТІВ-----------------}
{writeln ('ПІДМНОЖИНА   ---A----');}
   {for i:=1 to k1-1 do
      begin
       for j:=i+1 to k1 do
       write ('pa^[',i,',',j,']=',pa[i]^[j]:4:4,'  ');
      end;
      readln;}
{-------Виведення всієї матриці-------}
        {for i:=1 to k1 do
         begin
          for j:=1 to k1 do
           begin
           pa[j]^[i]:=pa[i]^[j];
           write ('pa^[',i,',',j,']=',pa[i]^[j]:4:4,'  ');
           end;
         end;
          readln;}
{writeln ('ПІДМНОЖИНА   ---B----');}
         {for i:=1 to k1-1 do
          begin
           for j:=i+1 to k1 do
           write ('pb^[',i,',',j,']=',pb[i]^[j]:4:4,'  ');
          end;
           readln;}
{------- Виведення всієї матриці -------}
```

```
{          for i:=1 to k1 do
          begin
           for j:=1 to k1 do
            begin
            pb[j]^[i]:=pb[i]^[j];
            write ('pb[',i,',',j,']=',pb[i]^[j]:4:4,'  ');
            end;
          end;
           readln;}
{процедура сортування підмножин A и B }
Sor_1AB (pa,sora); {процедура сортування елементів підмножини A}
{------------------- ВИВЕДЕННЯ РЕЗУЛЬТАТІВ --------------------}
{writeln ('РЕЗУЛЬТАТ СОРТУВАННЯ МНОЖИНИ ----A-----');}
   {for i:=1 to sz do
    begin
 Stop_Kadr (i);
     writeln ('sora[',i,']=',sora[i]:4:4);
    end;
     readln;}

GETMEM (zA, SizeOf(te6));
Dip_AB (sora,pa,zA); {процедура формування диполей матриці -----A------}
{---------- ВИВЕДЕННЯ РЕЗУЛЬТАТІВ -------------------}
{writeln (' формування диполей підмножини ----A-----');}
kd1:=(k1*k1-k1) div 2;
{for j:=1 to kd1 do
     begin
      Stop_Kadr1 (j);
      writeln ('Адрес диполя =',j,'--------------');
     write ('-zA[1,',j,']=',zA^[1,j],'   ');
     write ('-zA[2,',j,']=',zA^[2,j],'   ');
     writeln ('-----');
     end;
     readln;}
Sor_1AB (pb,sorb); {процедура сортування елементів підмножини   B}
 {--------- ВИВЕДЕННЯ РЕЗУЛЬТАТІВ --------------------}
{writeln ('РЕЗУЛЬТАТ СОРТУВАННЯ МНОЖИНИ -----B-----');}
kd1:=(n*n-n) div 2;
   {for i:=1 to sz do
    begin
     Stop_Kadr (i);
     writeln (' sorb[',i,']=',sorb[i]:4:4);
    end;
     readln;}
GETMEM (zB, SizeOf(te6));
Dip_AB (sorb,pb,zB); {процедура формування диполей матриці -----B------}
 {--------- ВИВЕДЕННЯ РЕЗУЛЬТАТІВ --------------------}
{writeln (' формування диполей підмножини ----B-----');}
kd1:=(k1*k1-k1) div 2;
{for j:=1 to kd1 do
     begin
      Stop_Kadr1 (j);
```

```
      writeln ('Адрес диполя =',j,'--------------');
     write ('-zB[1,',j,']=',zB^[1,j],'   ');
     write ('-zB[2,',j,']=',zB^[2,j],'   ');
     writeln ('-----');
     end;
     readln;}
{writeln (MemAvail, ' Байт вільно на початку процедури формування дерева A');
readln;}
Derevo_AB (zA,kd1,k1,bA); {процедура формування дерева A}
clrscr;
 {--------- ВИВЕДЕННЯ СФОРМОВАНОГО ДЕРЕВА   A ----------}
{writeln('Зформоване дерево підмножини A має вид ');}
              k:=0;
              for i:=1 to kd1-1 do
               begin
                s:=0;
                  for j:=1 to k1 do
                   s:=s+bA[i]^[j];
                    if s<>0 then  begin
                    k:=k+1;
                    getmem(bA1[k],k1*sizeof(integer));
                    bA1[k]^[j]:=0;
                    for j:=1 to k1 do
                    for j:=1 to k1 do
                     begin
                    bA1[k]^[j]:=bA[i]^[j]; {Stop_Kadr1 (k);}
                    {write('  ',bA1[k]^[j]);}
                     end;
                    {writeln ('    k=',k,'  ');}
                              end;
               end;
               {readln;}
                  {запис в файл значення дерева A}
                  {ASSIGN (f2,'d:\Work_pr\Klast1f4\PodA');}
                  REWRITE (f2);
                  for i:=1 to k do
                   begin
                    for j:=1 to k1 do
                     begin
                      if j=k1 then
                      writeln (f2,'  ',bA1[i]^[j]) else
                      write (f2,'  ',bA1[i]^[j]);
                      end;
                    end;
Derevo_AB (zB,kd1,k1,bB); {процедура формування дерева B}
clrscr;
 {---------ВИВЕДЕННЯ СФОРМОВАНОГО ДЕРЕВА B ----------}
{writeln('Сформоване дерево підмножини B має вид ');}
              k:=0;
              for i:=1 to kd1-1 do
               begin
                s:=0;
```

```
                for j:=1 to k1 do
                 s:=s+bB[i]^[j];
                  if s<>0 then begin
                  k:=k+1;
                  getmem(bB1[k],k1*sizeof(integer));
                  bB1[k]^[j]:=0;
                  for j:=1 to k1 do
                  for j:=1 to k1 do
                   begin
                  bB1[k]^[j]:=bB[i]^[j]; {Stop_Kadr1 (k);}
                  {write('  ',bB1[k]^[j]);}
                   end;
                  {writeln ('    k=',k,'  ');}
                            end;
              end;
              {readln;}
                 {запис в файл значення дерева B}
                 {ASSIGN (f3,'d:\Work_pr\Klast1f4\PodB');}
                 REWRITE (f3);
                 for i:=1 to k do
                  begin
                   for j:=1 to k1 do
                    begin
                     if j=k1 then
                     writeln (f3,'  ',bB1[i]^[j]) else
                     write (f3,'  ',bB1[i]^[j]);
                     end;
                   end;
KRIT (bA1,bB1,k1,cy1);
   i2:=0;
 for i:=k1-1{1} downto 2 do
  begin
   i2:=i2+1;
   {writeln ('Коеф. непротиречивості CY[',i,' класт.]=',cy1[i2]:4:4);
   readln;}
   Append(f3);
   writeln (f3, 'Коеф. непротиречивості CY[',i,' класт.]=',cy1[i2]:4:4);
  end;
{---перевірка значення cy1=0 на предмет проведення подальшої регуляризації}
 clrscr;
 {writeln (               'Коеф.непротиречивості равен 0');
 writeln (              '-------------------------------');}
 ost2:=0;
 for i:=k1-{1}2 downto 1 do
  begin
   if cy1[i]=0 then
    begin
     ost2:=ost2+1;
     writeln ('Коеф. непротиречивості CY[',i,']=',cy1[i]:4:4);
     {readln}
     ost:=0;{змінна зупинки}
    end
```

```
   end;
   if (ost2=1) and (ost=0) then readln;
{-----------------------------------------------------}
 {writeln (MemAvail, ' Байт вільно в кінці програми');
 readln;}
 FREEMEM (zA, SizeOf(te6));
 FREEMEM (zB, SizeOf(te6));

 for i:=1 to kd1 do begin
 FREEMEM (bA[i], kd1*sizeof(integer));
 FREEMEM (bB[i], kd1*sizeof(integer));
                 end;

 for i:=1 to k do begin
 FREEMEM (bA1[i], k1*sizeof(integer));
 FREEMEM (bB1[i], k1*sizeof(integer));
               end;

 for i:=1 to k1-1 do
  begin
   FREEMEM (pa[i],{sizeof(te7)}k1*sizeof(real));
   FREEMEM (pb[i],{sizeof(te7)}k1*sizeof(real));
  end;
 {writeln (MemAvail, ' Байт вільно в кінці циклу довизначення);
 readln;}

 ost1:=ost1+1;
 until ((((ost=0) and (ost2=1))) or (ost1=r1));
 {end;{кінець циклу по r1 -- довизначення }
 CLOSE (f1);
 close(f2);
 close(f3);
 for i:=1 to n  do
 FREEMEM (m[i], n*sizeof(real));

 writeln (MemAvail, 'Байт вільно після очистки');
 readln;

END.
```

Додаток Д.

Акти впровадження результатів дисертаційної роботи

ЗАТВЕРДЖУЮ
Заступник директора Інституту проблем математичних машин і систем НАН України
д.ф.-м.н., професор
_____ В.П. Клименко
"30" листопада 2020 року

АКТ

про впровадження результатів дисертаційного дослідження
Кузьменко Лідії Володимирівни

Даним актом засвідчується, що нижчеперелічені наукові положення, а саме:

технологія створення та вибору раціонального варіанту побудови автоматизованої системи управління (АСУ) типового ситуаційного центру (СЦ), яка поєднує в собі:

метод формування раціональної конфігурації прототипу АРМ типового СЦ;

метод вибору раціонального варіанту ПЗ прикладного рівня типового СЦ;

технологія визначення впливу загроз на процеси функціонування типового СЦ та оцінки стану його захищеності, яка поєднує в собі:

семантичну модель протиборства системи захисту СЦ та атакуючої сторони;

модель оцінки стану захищеності АСУ СЦ від кіберзагроз;

метод детектування та відновлення даних в СЦ, -

що розроблені Кузьменко Л.В, використано в Інституті проблем математичних машин і систем НАН України під час виконання у 2019 – 2020 роках за Державним контрактом від 09.08.2018 № 183/18/2 науково-дослідної роботи «Базис-Наука» (державний номер реєстрації 0119U000042дс), спрямованої на вирішення питань побудови мережі гарантоздатних СЦ сектору безпеки і оборони (СБО).

Отримані Л.В.Кузьменко результати було використано при дослідженні проблеми побудови різнорідних інформаційних систем (ІС) різних СЦ СБО та обміну даними між ними в контексті прийняття обґрунтованих рішень щодо вибору прототипу АРМ раціональної конфігурації та раціонального ПЗ прикладного рівня для комплектування АРМ та типового СЦ в цілому, відслідковування впливу шкідливих програм, завідомо фальшивого ПЗ і злоякісних шифруючих кодів на інформаційно-технологічні процеси в АСУ СЦ, а також оцінювання стану захищеності варіанту побудови АСУ СЦ від загроз порушення цілісності, конфіденційності і доступності та убезпечення від НСД до ресурсів СЦ та інформації, що в них циркулює.

Отримані автором результати дозволяють підвищити ефективність функціонування мережі гарантоздатних СЦ. В подальшому їх буде використано для побудови моделі взаємодії при створенні мережі СЦ органів державної влади, що дасть змогу об'єднати їх ІС в єдине інформаційне поле обміну даними та дозволить значно прискорити і спростити їх інтеграцію.

Завідувач відділу 235 ІПММС НАН України
к.т.н. _____ В.Ф. Гречанінов

ЗАТВЕРДЖУЮ
Начальник Національного центру управління
та випробувань космічних засобів
канд. техн. наук, старш. наук. співр.

Володимир ПРИСЯЖНИЙ

«17» грудня 2020 року

А К Т

про впровадження результатів дисертаційної роботи здобувача наукового ступеня кандидата технічних наук Кузьменко Лідії Володимирівни на тему «Інформаційна технологія для створення перспективних гарантоздатних автоматизованих систем управління об'єктами критичної інфраструктури»

Комісія Національного центру управління та випробувань космічних засобів у складі:

голови комісії - начальника відділу науково-дослідної та випробувальної роботи, канд. техн. наук Мамарєва В.М;

членів комісії:
- заступника начальника відділу науково-дослідної та випробувальної роботи, канд. техн. наук, старш. наук. співр. Козуба А.М.;
- головного фахівця відділу науково-дослідної та випробувальної роботи, канд. техн. наук Кутового О.М.;
- начальника відділу технічного захисту інформації Шпиталя О.О.

у період з «07» по «10» грудня 2020 року розглянула матеріали та результати дисертаційного дослідження Кузьменко Л.В. на тему «Інформаційна технологія для створення перспективних гарантоздатних автоматизованих систем управління об'єктами критичної інфраструктури»

КОМІСІЯ ВСТАНОВИЛА ТА ДАНИМ АКТОМ ЗАСВІДЧУЄ:

1) наукові положення, отримані особисто Кузьменко Л.В., зокрема метод визначення впливу загроз на процеси функціонування перспективних гарантоздатних автоматизованих систем управління об'єктами критичної інфраструктури впроваджено Національним центром управління та випробувань космічних засобів в НДР «Розробка науково-технічних пропозицій з організації віддаленого управління станціями оптико-

електронних спостережень типу 1 та типу 2» (номер держ. реєстрації 0120U105420).

2) впровадження зазначених наукових положень в частині детектування та відновлення даних, зашифрованих внаслідок впливу шкідливих програм та зловмисних шифруючих кодів забезпечило:

- можливість реалізації процедури пошуку вразливостей або істинних значень ключів, застосованих для зловмисного шифрування даних;
- можливість реалізації процедури оцінювання стійкості криптосистем, що забезпечують цілісність та конфіденційність команд управління станціями оптико-електронних спостережень в режимі віддаленого доступу.

Економічний ефект від впровадження не розраховувався у зв'язку з науковим призначенням результатів.

Акт складено для представлення у спеціалізовану вчену раду та не є підставою для виплати винагороди за впровадження та інших авторських винагород.

Голова комісії: Віктор МАМАРЄВ

Члени комісії: Андрій КОЗУБ

Олександр КУТОВИЙ

Олександр ШПИТАЛЬ

ЗАТВЕРДЖУЮ
Начальник Департаменту інформаційної безпеки НЕК «Укренерго»,
кандидат технічних наук
_____ В.В. Єрмошин
" 4 " січня 2021 року

АКТ
про впровадження результатів дисертаційного дослідження
Кузьменко Лідії Володимирівни

Даним актом засвідчується, що нижчеперелічені наукові положення, розроблені Л.В. Кузьменко, а саме:

1) метод формування типового варіанту побудови перспективної гарантоздатної АСУ об'єкту критичної інфраструктури;
2) метод визначення впливу загроз на процеси функціонування перспективної гарантоздатної АСУ об'єкту критичної інфраструктури, -

використано в НЕК «Укренерго» під час виконання робіт зі створення та розгортання інформаційно-телекомунікаційних систем (ІТС) для потреб її структурних підрозділів, а також при налаштуванні SIEM систем, спрямованих на вирішення завдань захисту таких ІТС від сучасних кіберзагроз.

Інноваційний підхід щодо **формування типового варіанту побудови перспективної гарантоздатної (ПГ) АСУ об'єкту критичної інфраструктури (ОКІ)**, який в інтерпретації Кузьменко ЛВ. базується на *процедурах вибору прототипу топології мережевої інфраструктури, формування раціональної конфігурації типового АРМ, раціонального вибору ПЗ прикладного рівня та власне процедурі вибору типового варіанту побудови ПГ АСУ* **дозволив**, як результат, скоротити час на вибір типової ІТС для потреб структурних підрозділів НЕК «Укренерго» з відповідним технічним і програмним забезпеченням та впровадження такої ІТС на існуючій в НЕК «Укренерго» мережі приблизно на 18 - 20%.

Розроблення Кузьменко Л.В. в межах методу **визначення впливу загроз на процеси функціонування ПГ АСУ ОКІ** *семантичної моделі протиборства системи захисту та атакуючої сторони, моделі оцінки стану захищеності АСУ від кіберзагроз та процедури детектування та відновлення даних, спотворених внаслідок впливу шкідливих програм, фальшивого ПЗ і зловмисних шифруючих кодів* **дозволило**, як результат, за рахунок оперативного визначення найбільш значимих загроз, своєчасного реагування на стан захищеності ІТС від загроз порушення цілісності, конфіденційності та доступності, а також проведення низки організаційно-правових заходів, - підвищити ефективність дій осіб, відповідальних за забезпечення безпеки ІТС структурних підрозділів НЕК «Укренерго» приблизно на 12% та убезпечити ресурси ІТС й інформацію, що в них циркулює від несанкціонованого доступу.

Начальник відділу впровадження та
контролю процесів інформаційної безпеки
к.т.н. Я.В. Рой

Підпис Рой Я.В. засвідчую!
Провідний фахівець з обліку персоналу групи адміністрування та обліку персоналу відділу адміністрування та обліку персоналу Дирекції управління персоналом
«11» 01 2021 р.

ДОКУМЕНТ ПІДПИСАНО КЕП
Сертифікат 2B6C7DF9A3891DA104000000778A280001A57501
Підписувач РОЙ ЯНІНА ВОЛОДИМИРІВНА
Дійсний з 03.04.2020 10:50:28 по 03.04.2021 23:59:59

НЕК "Укренерго"
Вн.№ А-309 від 04.01.2021
сторінок 2 | сторінка 1

УТВЕРЖДАЮ
Проректор по науке и технике
Азербайджанского Технического Университета
_____ проф. И.Т. Пирмамедов
«05» января 2021 г.

АКТ

об использовании результатов кандидатской диссертации Кузьменко Лидии Владимировны по теме «Информационная технология для создания перспективных гарантоспособных автоматизированных систем управление объектами критической инфраструктуры»

Комиссия в составе: председатель – заведующим отделом «Магистратуры и докторантуры» Азербайджанского технического университета, к.т.н., доцент М.Ф.Гараев и члены комиссии - заведующий кафедрой «Компьютерные системы и сети», д.т.н., проф. В.А.Касымов, заведующий кафедрой «Информационные технологии и программирование», к.т.н., доцент З.А.Джафаров, д.т.н., профессор кафедры «Телекоммуникация и информационная безопасность» Т.М.Мансуров составили настоящий акт о том, что результаты диссертационной работы

-метод формирования типового варианта построения перспективной гарантоспособной (ПГ) автоматизированной системы (АС) обработки информации и управления, усовершенствованный путем внедрения процедуры выбора прототипа топологии сетевой инфраструктуры, процедуры формирования рациональной конфигурации типового АРМ и процедуры рационального выбора программных средств прикладного уровня;

-метод определения уровня влияния угроз на процессы функционирования перспективной гарантоспособной автоматизированной системы обработки информации и управления, усовершенствованный путем внедрения семантической модели противоборства системы защиты ПГ АС с атакующей стороной, алгоритма детектирования и восстановления данных в ПГ АС, а также модели оценки состояния защищенности ПГ АС от угроз нарушение целостности, конфиденциальности и доступности, разработаны лично автором и

использованы при преподавании дисциплин «Методы и средства информационной безопасности» и «Методы и технологии защиты телекоммуникационных сетей и систем» для магистрантов по специализации «Информационная безопасность телекоммуникационных систем» специальности 050627 - «Инженерия электроники, телекоммуникации и радиотехники» Азербайджанского Технического Унивеситета.

Их применение позволило повысить эффективность создания и внедрения новейших беспроводных технологий, обеспечить увеличение устойчивости и гарантоспособности беспроводных систем к воздействию антропогенных и техногенных угроз, а также повысить достоверность оценки состояния систем защиты беспроводных сетей в условиях воздействия вредных программ, програмного обеспечения и злокачественных шифрующих кодов.

Полученные соискателем результаты могут быть использованы при создании перспективных гарантоспособных автоматизированных систем обработки информации, а также высших учебных заведениях в процессе подготовки соответствующих образовательных компонент.

Председатель комиссии:
Зав. отделом, к.т.н., доцент _____ М.Ф. Гараев

Члены комиссии:
Заведующий кафедрой,
д.т.н., профессор _____ В.А. Касымов

Заведующий кафедрой,
к.т.н., доцент _____ З.А. Джафаров

Д.т.н., профессор _____ Т.М. Мансуров

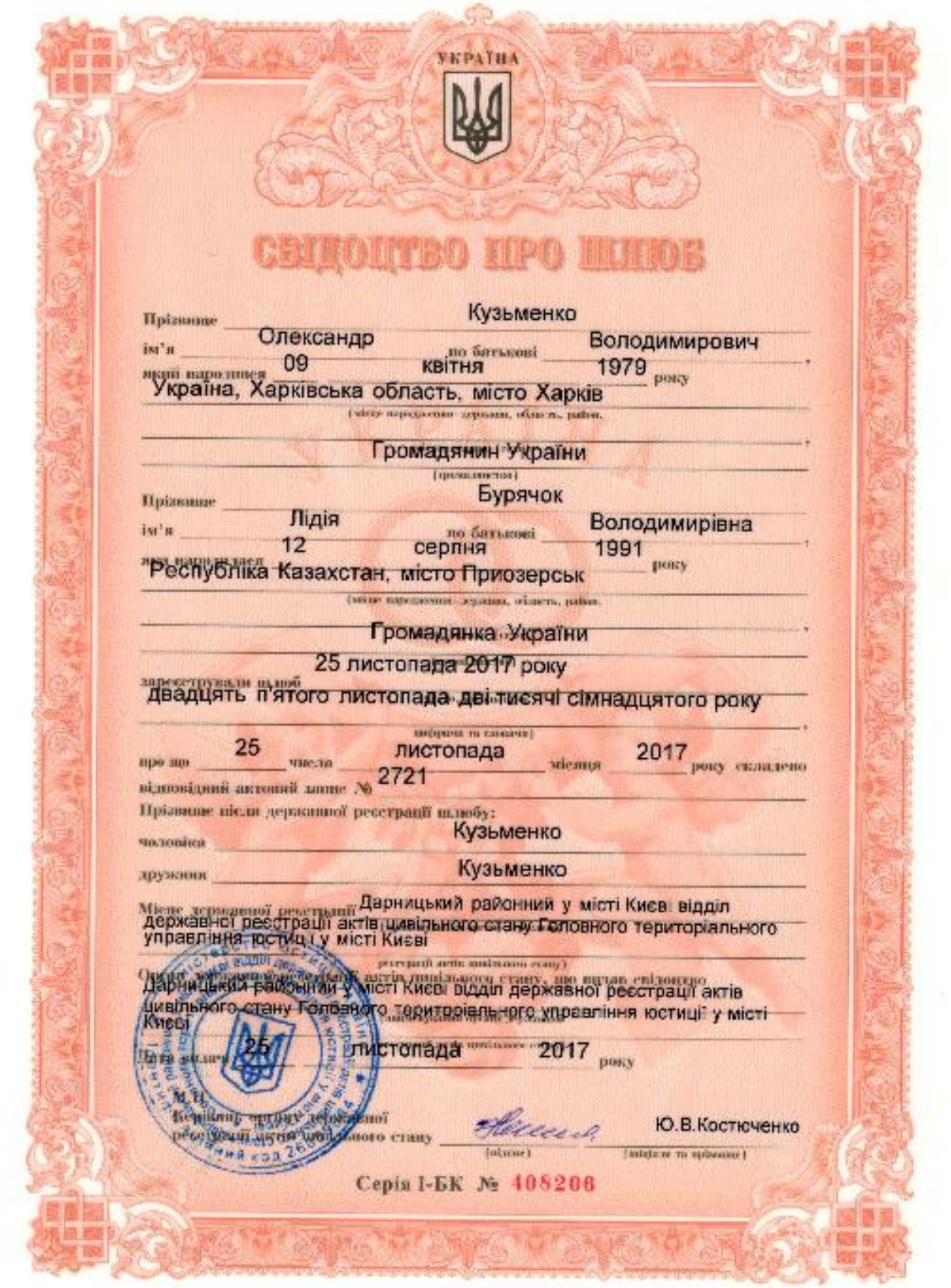
Додаток Е.

Відомості про апробацію результатів дисертаційної роботи

№ з/п	Назви конференції, конгресу, симпозіуму, семінару, школи	Місце та дата проведення	Форма участі	Де опубліковано
1	V-а НПК «Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення»	м. Київ, ВІТІ НТУУ "КПІ" МО України, 20-21.10.2010	Очна, тези доповіді	Доповіді та тези доповідей конференції
2	НПК «Проблеми кібербезпеки інфрормаційно-телекомунікаційних систем»	м. Київ, КНУ імені Т.Г. Шевченка, 10-11.03.2016	Очна, тези доповіді	Матеріали доповідей конференції
3	Регіональній конференції МСЕ для країн СНД та Грузії «Перспективи надання послуг на основі мереж пост-NGN, 4G и 5G. Організаційні і технічні рішення щодо їх побудови та захисту»	м. Київ, Державний університет телекомунікацій, 07-09.06.2017	Очна, доповідь	Тезиси доповідей конференції
4	НТК «Проблеми кібербезпеки інфрормаційно-телекомунікаційних систем»	м. Київ, КНУ імені Т.Г. Шевченка, 05-06.04.2018	Очна, тези доповіді	Матеріали доповідей конференції
5	VIII International conferece of students, PHD-students and young scientists «Engineer of XXI Century»	University of Belsko-Biala, Poland, 07.12.2018	Очна, доповідь	Колективна монографія в іноземному науковому виданні
6	X International conferece of students, PHD-students and young scientists «Engineer of XXI Century» http://www.engineerxxi.ath.eu/en/conference/	University of Belsko-Biala, Poland, 11.12.2020	online, постерна доповідь	Колективна монографія в іноземному науковому виданні

Додаток Ж.

Копія свідоцтва про укладення шлюбу (зміну прізвища)



УКРАЇНА

СВІДОЦТВО ПРО ШЛЮБ

Прізвище Кузьменко

ім'я Олександр по батькові Володимирович

який народився 09 квітня 1979 року

Україна, Харківська область, місто Харків

(місце народження: держава, область, район)

Громадянин України

(громадянство)

Прізвище Бурячок

ім'я Лідія по батькові Володимирівна

яка народилася 12 серпня 1991 року

Республіка Казахстан, місто Приозерськ

(місце народження: держава, область, район)

Громадянка України

зареєстрували шлюб 25 листопада 2017 року

двадцять п'ятого листопада дві тисячі сімнадцятого року

(цифрами та словами)

про що 25 числа листопада місяця 2017 року складено

відповідний актовий запис № 2721

Прізвище після державної реєстрації шлюбу:

чоловіка Кузьменко

дружини Кузьменко

Місце державної реєстрації Дарницький районний у місті Києві відділ державної реєстрації актів цивільного стану Головного територіального управління юстиції у місті Києві

(повне найменування органу державної реєстрації актів цивільного стану)

Орган, який видав свідоцтво про державну реєстрацію актів цивільного стану, що видав свідоцтво Дарницький районний у місті Києві відділ державної реєстрації актів цивільного стану Головного територіального управління юстиції у місті Києві

Дата видачі 25 листопада 2017 року

М.П.

Керівник органу державної реєстрації актів цивільного стану (підпис) Ю.В.Костюченко (ініціали та прізвище)

Серія І-БК № 408206