Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Міністерство освіти і науки України

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Міністерство освіти і науки України

Кваліфікаційна наукова праця

на правах рукопису

УДК 004.056

ПОЛУЦИГАНОВА ВІКТОРІЯ ІГОРІВНА

ДИСЕРТАЦІЯ
МЕТОД ОЦІНКИ РИЗИКУ НА ОСНОВІ АНАЛІЗУ СТРУКТУРИ ЗВ'ЯЗКІВ ЗАГРОЗ ТА ВРАЗЛИВОСТЕЙ У КІБЕРСИСТЕМАХ

12 – Інформаційні технології

125 – Кібербезпека та захист інформації

Подається на здобуття наукового ступеня доктора філософії

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

_____ В. І. Полуциганова

Науковий керівник

Смирнов Сергій Анатолійович, кандидат фізико-математичних наук, старший науковий співробітник

Київ – 2024

АНОТАЦІЯ

Полуциганова В. І. Метод оцінки ризику на основі аналізу структури зв’язків загроз та вразливостей у кіберсистемах. – Кваліфікаційна праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії з галузі знань 12 – Інформаційні технології за спеціальністю 125 – Кібербезпека та захист інформації. – Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, 2024.

Методи оцінки ризиків є одним з ключових механізмів аналізу ефективності та рівня безпечності функціонування кібернетичних систем і визначення напрямків їх подальшого розвитку, що обумовлено складною структурою таких об’єктів. Зважаючи на те, що сьогодні майже в усіх сферах життя застосовуються інформаційні технології, методи оцінювання ризиків набувають все більшого значення для виявлення уразливостей інформаційних систем та потенційних загроз для їх безпечного функціонування. Результати відповідного аналізу дозволяють формувати та проводити комплекс заходів, які підвищують рівень безпеки системи та захищають її від зовнішніх та внутрішніх загроз.

Дисертаційну роботу присвячено розробці методу оцінювання ризиків кіберсистем на основі взаємозалежності між уразливостями та загрозами, а також складної структури цих зв’язків.

Порівняльний аналіз сучасних підходів та методів оцінювання ризику засвідчив, що ними не в повній мірі враховується така специфіка структури інформаційної системи, як її складність, що відображається на точності проведених на основі цих методів розрахунків.

За результатами дослідження зв’язків між виявленими загрозами та уразливостями, які притаманні сучасним кіберсистемам, установлено, що зв’язки між ними можуть мати небінарний характер, а також впливають на обсяг втрат внаслідок різного рівня сумісності як між уразливостями системи,

так і між окремими подіями при реалізації атак (несанкціонованого доступу до системи).

Виявлені недоліки сучасних підходів, що застосовуються для аналізу ризику у кіберсистемах, були скореговані під час розроблення узагальненого методу оцінки ризиків для систем складної структури.

Методи аналізу вразливостей та загроз безпеки кіберсистем, аналізу структури складних кіберсистем, оцінювання ризику, а також сучасний стан вивчення проблем, які досліджуються в дисертації, висвітлено в роботах таких вчених як Архіпов О.Є., Аткін Р. Х., Грайворонський М. В., Джонсон Д. Х., Касті Д. Л., Качинський А. Б., Ланде Д. В., Мохор В. В., Новіков О. М. та інших науковців.

Проведено огляд та здійснено порівняльний аналіз основних підходів та методів, на яких базується структурний аналіз системи загроз і вразливостей і які покладено в основу дисертаційного дослідження, а саме наступних напрямів: Q-аналіз, топологія, геометрія і аналіз симплеціальних комплексів.

Здійснено опис основних етапів життєвого циклу вразливостей у кіберсистемі. Розглянуто основні методи оцінювання ризику на основі підходів А. Вальда та Т. Байєса.

Проведено систематизацію підходів до виявлення та аналізу основних метрик для опису структури системи уразливостей та загроз у кіберсистемі. Установлено, що основними поняттями та ефективними моделями, які у повній мірі характеризують структуру складних систем, а також використовуються для розв’язання задач аналізу та синтезу системи, однозначного визначення процедури при проведенні оцінювання ризиків, являються локальні карти, структурне дерево та структурний граф симплеціального комплексу.

Здійснено структурний аналіз системи вразливостей та запропоновано класифікацію вразливостей, що дозволяє суттєво вплинути на формування комплексу превентивних заходів щодо попередження та подолання несприятливих наслідків реалізації загроз. Для опису властивостей та джерел

виникнення вразливостей використовувалась база даних широко відомих уразливостей інформаційної безпеки CVE.

У ході дисертаційного дослідження було розроблено загальні алгоритми переходу від довільної матриці інцидентності до симплеціального комплексу з подальшим визначенням структурного дерева та локальних карт. Запропоновано алгоритм прямого переходу від матриці інцидентності безпосередньо до структурного дерева та локальних карт у випадку, коли відсутня необхідність побудови симплеціального комплексу.

Розроблено алгоритм відновлення симплеціального комплексу із застосуванням інформації з локальних карт та структурного дерева. Розроблений метод дозволяє здійснити формалізований перехід від характеристик топології симплеціального комплексу до відповідних графів та навпаки. Запропонований алгоритм дозволяє більш точно визначити структуру складної системи та здійснити її всебічний детальний аналіз. Цей метод відображає зв’язки між класичним Q-аналізом та доданими структурними характеристиками, а також синтезом симплеціального комплексу на основі відомих структурних характеристик.

У ході дослідження проводились уточнення оцінок ймовірностей інцидентів та відповідних втрат. Класична байєсова формула розрахунку середніх втрат дозволяє врахувати сумісність та залежність несприятливих подій, але, при цьому зазвичай оцінка ймовірностей реалізації загроз виконується для ситуації окремих несумісних подій. У реальності можуть відбуватися сумісні реалізації вразливостей/загроз, що ускладнює оцінки ймовірності внаслідок виникнення сумісних та умовних ймовірностей. У випадку, коли вразливості інформаційної системи є незалежними, загальні збитки від їх сумісної реалізації розраховуються як сума збитків від окремих інцидентів. Але, у разі сумісної реалізації залежних уразливостей системи, загальна сума окремих втрат корегується (збільшується або зменшується) у залежності від характеру та специфіки їх зв’язків.

Доведено, що відомі структурні особливості симплеціального комплексу при оцінюванні ризику дозволяють ураховувати сумісність між загрозами чи вразливостями. Сумісність в цьому контексті означає, що деякі вразливості можуть реалізовуватися як одночасно, так і окремо в залежності від профілю атаки на інформаційну систему.

Доведено, що чим більш складним є зв'язок між окремими вразливостями, тим більший вклад сумісних компонентів у загальний ризик. Акцентовано увагу на тому, що при обрахунку загального ризику системи потрібно окремо враховувати «місця склеювання» (примикання) між ланцюгами симплексів. Оскільки ці місця є симплексами за визначенням, ризик, що відповідає ланцюгу, формується з ризиків від двох ланцюгів по місцю примикання. Він обчислюється як сума ризиків для двох ланцюгів мінус ризик для симплекса примикання, бо він врахований двічі — у складі кожного ланцюга окремо. Якщо примикання по симплексу відбувається для k ланцюгів разом, зрозуміло, що для компенсації кратності примикання потрібно віднімати від суми ризиків від ланцюгів ризик від симплексу множений на (k -1).

Оскільки інформація щодо структури примикання міститься у локальній карті та структурному графі симплеціального комплексу, вона може бути використана для розрахунку ризику безпосередньо з них. Тому загальну суму ризиків (по ланцюгах) запропоновано корегувати з урахуванням таких повторів для кожної вершині структурного дерева. Запропонований розрахунок ризику відрізняється від алгоритмів «згортання дерева» у теорії прийняття рішень тим, що працює з комплексом а не деревом, використовує підхід «включень та виключень», а також враховує відповідну кратність примикання.

Здійснено загальний аналіз системи загроз і вразливостей інформаційної системи типового об'єкту критичної інфраструктури. За допомогою структурного аналізу виявлено можливість сумісних реалізацій загроз, які

проявляються через складну структуру взаємозалежностей між уразливостями та загрозами.

Проведено класифікацію вразливостей на основі параметрів, наведених у дисертаційному дослідженні для системи загроз інформаційної системи визначеного об'єкта критичної інфраструктури. За результатами проведених обчислень отримано опис структури системи загроз та ризиків, який більш точно відповідає реальним параметрам досліджуваної системи.

Для проведення розрахунку ризиків зроблено припущення, що сумісна реалізація несприятливих подій, зокрема від кібератаки, є незалежною за втратами. Тому втрати розраховуються як сума, а ймовірність події як добуток.

Отриманий результат також підтверджує, що при проведенні розрахунків з використанням запропонованого методу розширеного Q-аналізу структурно-вкладені загрози не мають впливу на кінцевий результат оцінки загального рівня ризику. Для спрощення розрахунків ризику вплив на систему структурно-вкладених загроз рекомендовано ігнорувати. Практичне застосування запропонованого методу оцінювання ризику засвідчило, що у порівнянні із методом спрощеної лінійної оцінки, загальна оцінка ризик для досліджуваної інформаційної системи об'єкта критичної інфраструктури зменшується майже до 23,3% у залежності від розподілу загроз та профілю атак.

Метою дисертаційної роботи є розв'язання актуальної наукової задачі аналізу та синтезу моделей і методів оцінювання ризиків з врахуванням структурних властивостей сукупності зв'язків загроз та вразливостей кіберсистем, що дозволяє розробити процедуру побудови формули байєсівської оцінки ризику, виконати її аналіз та забезпечити уточнення оцінки ризику внаслідок врахування структури сумісності вразливостей системи.

Об'єкт: загрози і вразливості у складних кіберсистемах.

Предмет: оцінювання ризиків у складних кіберсистемах.

У дисертаційному дослідженні отримані такі наукові результати:

- Вперше побудовано модель зв’язків загроз та вразливостей у кіберсистемі у вигляді симплеціального комплексу, яка представляє складну структуру їх взаємозалежностей, для класифікації загроз і вразливостей та для оцінювання потенційних втрат і ризиків;
- Вперше розроблено алгоритми аналізу симплекційного комплексу та його синтезу на основі повного набору структурних характеристик комплексу;
- Вперше розроблено метод класифікації загроз та вразливостей у складній системі з урахуванням характеристик власної розмірності підсистем, їх примикання та наслідування, що дозволяє надійніше оцінювати ризики в кіберсистемі в залежності від варіантів атак;
- Розроблено процедуру побудови байєсівської оцінки ризику з врахуванням структури вразливостей системи та складеної функції втрат.

Всі теоретичні і практичні результати дисертаційної роботи у повній мірі висвітлено у статтях, опублікованих у фахових вітчизняних наукових виданнях, що входять до відповідного встановленого переліку. Виконано їх належну апробацію на міжнародних та всеукраїнських наукових конференціях.

У дисертаційному дослідженні розв’язана задача оцінювання ризику з урахуванням структурних особливостей зв’язків уразливостей та загроз у кіберсистемах.

Проаналізовано систему зв’язків між загрозами та вразливостями в сучасних складних кіберсистемах. Виявлено, що зв’язки між ними можуть мати небінарний характер та визначати різний рівень сумісності між загрозами при реалізації атак.

Проаналізовано методи структурного аналізу складних систем. Основним його інструментом визначено Q-аналіз, адже саме він дозволяє врахувати топологію взаємозв’язків між компонентами вразливостей та загроз у кіберсистемі.

Побудовано структурну модель сумісної реалізації загроз для кіберсистем. Розроблено основні алгоритми для побудови структурної моделі системи взаємозалежностей загроз та вразливостей на основі Q-аналізу. Визначено основні структурні характеристики системи для подальшого обрахунку ризиків.

У роботі структуровано інформацію про загрози та вразливості кіберсистем. Описано основні метрики оцінки взаємозалежностей між уразливостями та загрозами для їх подальшого використання при проведенні розрахунку оцінки загального ризику для системи.

Здійснено аналіз методів оцінювання складених функцій втрат від реалізації сумісних загроз. Визначено, що внаслідок подібних атак на кіберсистему має здійснюватися корегування величини суми окремих втрат системи з урахуванням специфіки взаємних зв'язків. У загальному випадку при реалізації незалежних загроз сумарний збиток є сумою збитків внаслідок реалізацій окремих подій, але у разі виявлення взаємозалежності відповідних уразливостей та загроз, цей показник корегується (збільшується або зменшується) у залежності від характеру та специфіки їх зв'язків.

На основі характеристик побудованих моделей, які відображають структурні особливості системи загроз, розроблено метод оцінювання ризику з урахуванням структурних особливостей системи та складених функцій втрат.

Проаналізовано можливості практичного застосування розробленого методу оцінювання ризику з урахуванням специфіки взаємозв'язку вразливостей та загроз для інформаційних систем: 1) хмарних середовищ та 2) об'єктів критичної інфраструктури, а також виконано відповідні розрахунки. Здійснено порівняння результатів, отриманих при розрахунках оцінки ризику із застосуванням розробленого методу розрахунку для систем складної структури, з результатами, отриманими при розрахунках за допомогою простої лінійної оцінки ризику.

Результати роботи впроваджено у навчальний процес навчально-наукового фізико-технічного інституту Національного технічного

університету України «Київський політехнічний інститут імені Ігоря Сікорського», що підтвержено довідкою про вровадження в додатку Б.

Моделі та методи розроблені в дисертації використані в Науково-дослідні роботі «Підтримка прийняття рішень в умовах невизначеності та конкурентної взаємодії» номер державної реєстрації 0124U001957, що підтверджує наукову та практичну цінність отриманих результатів дослідження.

Наукові напрацювання та пропозиції даного дослідження використані під час підготовки матеріалів до засідання Ради національної безпеки і оборони України з питання «Про стан справ у енергетичній сфері», рішення Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України (далі – НКЦК), а також у процесі розроблення Загальних правил обміну інформацією про кіберінциденти, затверджених рішенням НКЦК (акт впровадження результатів дисертаційного дослідження наведено в додатку Б).

За матеріалами дисертації опубліковано 12 робіт, з яких 4 – це статті у журналах і збірниках наукових праць, що входять до переліку фахових видань, затверджених МОН України за спеціальністю дисертації та 8 – публікації у матеріалах конференцій (у тому числі, міжнародних).

Ключові слова: кібербезпека, інформаційна безпека, оцінка ризиків, Q-аналіз, симплекс, складні системи, мережеві структури, кібератаки, загрози, вразливості, байєсові методи, теорія графів, класифікація вразливостей, критична інфраструктура.

ABSTRACT

Polutsyhanova V. Methods of analysis of risks in complex structure cyber systems. − Qualifying scientific work, the manuscript.

PhD thesis in the field of knowledge 12 Information Technology in specialty 125 Cyber security and information protection. – National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Kyiv, 2024.

Risk assessment methods are one of the key mechanisms for analyzing the effectiveness and safety level of the functioning of cybernetic systems and determining the direction of their further development, which is due to the complex structure of such objects. Given the fact that information technologies are used in almost all spheres of life today, risk assessment methods are becoming more and more important for identifying vulnerabilities of information systems and potential threats to their safe functioning. The results of the relevant analysis make it possible to form and carry out a set of measures that increase the level of system security and protect it from external and internal threats.

The dissertation work is devoted to the development of a method for assessing the risks of cyber systems based on the interdependence between vulnerabilities and threats, as well as the complex structure of these connections.

A comparative analysis of modern risk assessment approaches and methods proved that they do not fully take into account the specifics of the structure of the information system, such as its complexity, which is reflected in the accuracy of the calculations based on these methods.

According to the results of the study of the connections between the detected threats and vulnerabilities that are inherent in modern cyber systems, it was established that the connections between them can be non-binary in nature, and also affect the amount of losses due to different levels of compatibility both between system vulnerabilities and between individual events when implementing attacks (unauthorized access to the system). Identified shortcomings of modern approaches used for risk analysis in cyber systems were corrected during the development of a generalized risk assessment method for systems with a complex structure.

The methods of analyzing the vulnerabilities and security threats of cyber systems, analyzing the structure of complex cyber systems, risk assessment, as well as the current state of studying the problems investigated in the dissertation, are covered in the works of such scientists as O. Ye. Arkhipov, R. Kh. Atkin, M. V. Graivoronsky ., Johnson D.H., Casti D.L., Kaczynskiy A.B., Lande D.V., Mohor V.V., Novikov O.M. and other scientists.

An overview and a comparative analysis of the main approaches and methods, which are based on the structural analysis of the system of threats and vulnerabilities and which are the basis of the dissertation research, were carried out, namely the following areas: Q-analysis, topology, geometry and analysis of simplicial complexes.

The description of the main stages of the life cycle of vulnerabilities in the cyber system is carried out. The main methods of risk assessment based on the approaches of A. Wald and T. Bayes are considered.

Systematization of approaches to the detection and analysis of the main metrics for describing the structure of the system of vulnerabilities and threats in the cyber system has been carried out. It was established that the main concepts and effective models that fully characterize the structure of complex systems, and are also used to solve the problems of system analysis and synthesis, unambiguous definition of the procedure for risk assessment, are local maps, a structural tree, and a structural graph of a simplicial complex .A structural analysis of the system of vulnerabilities was carried out and a classification of vulnerabilities was proposed, which allows to significantly influence the formation of a set of preventive measures to prevent and overcome the adverse consequences of the implementation of threats. The CVE database of widely known information security vulnerabilities was used to describe the properties and sources of vulnerabilities.

In the course of the dissertation research, general algorithms for the transition from an arbitrary incidence matrix to a simplicial complex were developed, followed by the definition of a structural tree and local maps. An algorithm for

direct transition from the incidence matrix directly to the structural tree and local maps is proposed in the case when there is no need to build a simplicial complex.

An algorithm for restoring the simple complex using information from local maps and a structural tree has been developed. The developed method makes it possible to carry out a formalized transition from the characteristics of the topology of the simplicial complex to the corresponding graphs and vice versa. The proposed algorithm makes it possible to more accurately determine the structure of a complex system and carry out its comprehensive detailed analysis. This method reflects the connections between classical Q-analysis and added structural features, as well as symplectial complex synthesis based on known structural features.

In the course of the study, estimates of the probability of incidents and corresponding losses were refined. The classic Bayesian formula for calculating average losses allows you to take into account the compatibility and dependence of adverse events, but at the same time, the assessment of the probabilities of the realization of threats is usually performed for the situation of individual incompatible events. In reality, compatible implementations of vulnerabilities/threats may occur, which makes it difficult to estimate the probability due to the occurrence of compatible and conditional probabilities. In the case when the vulnerabilities of the information system are independent, the total losses from their joint implementation are calculated as the sum of losses from individual incidents. But, in the case of the joint implementation of dependent system vulnerabilities, the total amount of individual losses is adjusted (increased or decreased) depending on the nature and specificity of their connections.

It has been proven that the known structural features of the symplectial complex make it possible to take into account compatibility between threats or vulnerabilities during risk assessment. Compatibility in this context means that some vulnerabilities can be implemented both simultaneously and separately, depending on the profile of the attack on the information system.

It has been proven that the more complex the relationship between individual vulnerabilities, the greater the contribution of compatible components to the overall

risk. Attention is focused on the fact that when calculating the overall risk of the system, it is necessary to separately take into account the "gluing places" (joining) between the chains of simplexes. Since these locations are simplexes by definition, the risk corresponding to the chain is formed from the risks of the two chains at the junction.It is calculated as the sum of the risks for two chains minus the risk for the adjacency simplex, because it is taken into account twice - as part of each chain separately. If simplex connection occurs for k chains together, it is clear that to compensate for the multiplicity of connections, the simplex risk multiplied by (k -1) must be subtracted from the sum of risks from the chains.

Since the information about the adjacency structure is contained in the local map and the structural graph of the simplicial complex, it can be used to calculate the risk directly from them. Therefore, the total amount of risks (by chains) is proposed to be adjusted taking into account such repetitions for each vertex of the structural tree. The proposed risk calculation differs from the "tree collapse" algorithms in decision-making theory in that it works with a complex rather than a tree, uses an "inclusions and exclusions" approach, and also takes into account the appropriate multiplicity of adjacency.

A general analysis of the system of threats and vulnerabilities of the information system of a typical object of critical infrastructure was carried out. With the help of structural analysis, the possibility of compatible implementations of threats was revealed, which are manifested through a complex structure of interdependencies between vulnerabilities and threats.

The classification of vulnerabilities was carried out based on the parameters given in the dissertation study for the threat system of the information system of the specified critical infrastructure object. Based on the results of the calculations, a description of the structure of the system of threats and risks was obtained, which more accurately corresponds to the real parameters of the studied system.In order to calculate the risks, it is assumed that the joint realization of adverse events, in particular from a cyber attack, is independent of losses. Therefore, losses are calculated as a sum, and the probability of an event as a product.

The obtained result also confirms that when performing calculations using the proposed method of extended Q-analysis, structurally nested threats do not have an impact on the final result of the assessment of the overall level of risk. To simplify risk calculations, it is recommended to ignore the impact on the system of structurally embedded threats. The practical application of the proposed risk assessment method proved that, compared to the simplified linear assessment method, the overall risk assessment for the studied information system of the critical infrastructure object is reduced to almost 23.3%, depending on the distribution of threats and attack profile.

The aim of the dissertation is to solve the current scientific problem of analysis and synthesis of risk assessment models and methods, taking into account the structural properties of the set of threats and vulnerabilities of cyber systems, which allows to develop a procedure for building a Bayesian risk assessment formula, perform its analysis and ensure the refinement of risk assessment due to taking into account the compatibility structure of system vulnerabilities.

Object: threats and vulnerabilities in complex cyber systems.

Subject: risk assessment in complex cyber systems.

The following scientific results were obtained in the dissertation research:

– For the first time, a model of the links between threats and vulnerabilities in the cyber system was built in the form of a simplicial complex, which represents a complex structure of their interdependencies, for the classification of threats and vulnerabilities and for assessing potential losses and risks;

– Algorithms for the analysis of the symplectic complex and its synthesis based on a complete set of structural characteristics of the complex were developed for the first time;

– For the first time, a method of classifying threats and vulnerabilities in a complex system was developed, taking into account the characteristics of the subsystems' own dimensions, their adjacency and imitation, which allows for a more reliable assessment of risks in the cyber system depending on the attack options;

– A procedure for constructing a Bayesian risk assessment was developed, taking into account the structure of system vulnerabilities and the composite loss function.

All theoretical and practical results of the dissertation work are fully covered in articles published in specialized domestic scientific publications, which are included in the corresponding established list. They have been properly approved at international and all-Ukrainian scientific conferences.

The dissertation research solves the problem of risk assessment taking into account the structural features of connections between vulnerabilities and threats in cyber systems.

The system of connections between threats and vulnerabilities in modern complex cyber systems is analyzed.It was found that the connections between them can have a non-binary nature and determine a different level of compatibility between threats in the implementation of attacks.

Methods of structural analysis of complex systems are analyzed. Its main tool is defined as Q-analysis, because it allows taking into account the topology of relationships between the components of vulnerabilities and threats in the cyber system.

A structural model of the compatible implementation of threats to cyber systems has been built. Basic algorithms for building a structural model of the system of interdependencies of threats and vulnerabilities based on Q-analysis have been developed. The main structural characteristics of the system are determined for further calculation of risks.

Information about threats and vulnerabilities of cyber systems is structured in the work. The main metrics for assessing the interdependencies between vulnerabilities and threats are described for their further use when calculating the overall risk assessment for the system.

An analysis of methods for estimating composite functions of losses from the implementation of compatible threats was carried out. It was determined that as a result of such attacks on the cyber system, the amount of individual losses of the

system should be adjusted, taking into account the specifics of mutual connections. In the general case, when independent threats are implemented, the total damage is the sum of losses due to the implementation of individual events, but in case of detection of interdependence of relevant vulnerabilities and threats, this indicator is adjusted (increased or decreased) depending on the nature and specificity of their connections. Based on the characteristics of the built models, which reflect the structural features of the threat system, a risk assessment method was developed taking into account the structural features of the system and composite loss functions.

The possibilities of practical application of the developed risk assessment method were analyzed, taking into account the specifics of the relationship between vulnerabilities and threats to information systems: 1) cloud environments and 2) critical infrastructure objects, and corresponding calculations were performed. A comparison of the results obtained during risk assessment calculations using the developed calculation method for systems of a complex structure with the results obtained during calculations using a simple linear risk assessment was made.

The results of the work have been incorporated into the educational process of the educational-scientific physical and technical institute of the National Technical University of Ukraine "Ihor Sikorskyi Kyiv Polytechnic Institute".

The models and methods developed in the dissertation are used in the research and development work "Supporting decision-making in conditions of uncertainty and competitive interaction" state registration number 0124U001957, which confirms the scientific and practical value of the obtained research results.

Scientific developments and proposals were used during the preparation of materials for the meeting of the National Security and Defense Council of Ukraine on the issue "On the state of affairs in the energy sector", the decision of the National Coordination Center for Cyber Security under the National Security and Defense Council of Ukraine (hereinafter - the National Security and Defense Council of Ukraine), as well as in the process development of the General Rules for

the exchange of information on cyber incidents, approved by the decision of the NCCC.

12 works have been published based on the dissertation materials, of which 4 are articles in journals and collections of scientific works that are included in the list of specialized publications approved by the Ministry of Education and Science of Ukraine for the dissertation specialty, and 8 are publications in the materials of conferences (including international ones).

Keywords: cyber security, information security, risk assessment, Q-analysis, simplex, complex systems, network structures, cyber attacks, threats, vulnerabilities, Bayesian methods, graph theory, vulnerability classification, critical infrastructure.

List of principal publications of the applicant:

1. Полуциганова В. І., Смирнов С. А. Методологія побудови основних метрик q-аналізу та їх застосування. *Системні дослідження та інформаційні технології*. 2019. № 3. С. 76 – 88. URL: https://doi.org/10.20535/srit.2308-8893.2019.3.07 (date of access: 10.11.2023).

У роботі здобувачем впроваджено такі поняття, як структурне дерево, локальні карти та процедура наслідування, які дозволяють роз'яснити сенс метрик системи, отриманих за допомогою Q-аналізу. На цій основі розроблено алгоритми для визначення основних метрик системи, які застосовано до банківської системи.

2. Polutsyganova V., Smirnov S. The inverse problem of Q-analysis of complex systems structure in cyber security. Theoretical and applied cybersecurity. 2023. Vol. 4, no. 1. P. 61 – 68. URL: https://doi.org/10.20535/tacs.2664-29132022.1.274123 (date of access: 10.11.2023).

У роботі здобувачем наведено розроблений алгоритм відновлення або синтезу симплеціальних комплексів з елементарного набору симплексів за допомогою локальних бінарних карт і структурного дерева. Цей алгоритм використовується для зменшення обсягу даних, які необхідно зберігати для

характеристики системи, якщо комплекс описує велику складну систему таку, як система кібербезпеки.

3. Polutsyhanova V. I. System construction of cybersecurity vulnerabilities with Q-analysis. *Theoretical and applied cybersecurity*. 2023. Vol. 5, no. 1. P. 52-55. URL: https://doi.org/10.20535/tacs.2664-29132023.1.285430.

У роботі здобувачем запропоновано метод, який дозволяє будувати моделі складних систем на основі їх уразливостей з урахуванням прихованих зв'язків. При цьому, наведено можливості Q-аналізу для дослідження структури системи взаємопов'язаних уразливостей, які виникають в процесі реалізації проекту. Наведено приклад застосування методів Q-аналізу та запропоновано пояснення природного стану системи, а також впливу деяких потенційних загроз та їх комбінацій.

4. Polutsyhanova V. I. Vulnerability classification using Q-analysis. *Theoretical and applied cybersecurity*. 2023. Vol. 5, no. 2. P. 56–61.

У роботі здобувачем представлено метод розрахунку оцінки ризиків для систем складної структури та наведено приклад побудови, аналізу та класифікації вразливостей залежно від загроз, які вони породжують. Такий підхід висвітлює зв'язки та сумісну реалізацію між уразливими місцями, а також ступінь впливу кожної з них на рівень загроз.

5. Медведенко (Полуциганова) В. І., Смирнов С. А. Використання q-аналізу для дослідження зв'язків у банківських системах. *XV Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики»*: Всеукр. науково-практ. конференція студентів, аспірантів та молодих вчен., м. Київ, 25–27 трав. 2017 р. Київ, 2017. С. 44–46.

У роботі здобувачем наведено результати досліджень взаємозв'язку уразливостей від загроз, які вони породжують, для інформаційної системи банківських установ за допомогою Q-аналізу. Проведено пошук зв'язків вищих порядків у досліджуваній системі та надані рекомендації для практичного

застосування результатів у процесах прийняття рішень для посилення інформаційної безпеки в банківських установах.

6. Медведенко (Полуциганова) В. І., Смирнов С. А. Використання алгоритмів q-аналізу на прикладі банківської системи. *XVI Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики»*: Всеукр. науково-практ. конференція студентів, аспірантів та молодих вчен., м. Київ, 26–27 квіт. 2018 р. Київ, 2018. С. 33–36.

У роботі здобувачем представлено розроблені алгоритми Q-аналізу для систем з великою кількістю елементів та описано їх застосування на прикладі інформаційної системи банківської установи. Проведено аналіз результатів роботи алгоритмів, надані рекомендації для їх використання в процесах прийняття рішень щодо посилення інформаційної безпеки в банківських установах.

7. Polutsyhanova V. The inverse problem of q-analysis. *XVIII Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики»:* Всеукр. науково-практ. конференція студентів, аспірантів та молодих вчен., м. Київ, 12–13 трав. 2020 р. С. 113–115.

У роботі здобувачем запропоновано метод відновлення симплеціальних комплексів з елементарного симплексу за допомогою локальних карт і структурного дерева. Цей метод зменшує обсяг даних, що зберігаються, і покращує процес управління, якщо комплекс описує складну систему.

8. Полуциганова В. І., Смирнов С. А. The inverse problem of Q-analysis of complex systems structure. *Інформаційні технології та безпека. Матеріали XXI міжнародної науково-практичної конференції. Випуск 22*, м. Київ, 2021. С. 114–118.

У роботі здобувачем висвітлено метод оберненої задачі Q-аналізу, тобто відновлення комплексу за допомогою локальних карт і структурного дерева. Представлено загальний приклад практичного використання.

9. Полуциганова В. І., Смирнов С. А. Оцінювання ризиків складних систем з використання методів Q-аналізу. *Інформаційні технології та безпека матеріали XXII міжнародної науково-практичної конференції*, м. Київ, 2022. С. 51–52.

У роботі здобувачем наведено розроблений метод оцінювання ризиків для структурно та функціонально складних систем, в яких уразливості, а як наслідок, і збитки від них, можуть реалізовуватись одночасно.

10. Полуциганова В. І., Смирнов С. А. Structure of vulnerability in complex systems and risk assessment// МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ «Виклики і загрози для критичної інфраструктури». 21-22 березня 2023 р. м. Київ, Україна. С. 334-335.

У роботі здобувачем представлено розроблену методику оцінки ризиків для структурно-функціональної складності інформаційних систем, в якій уразливості можуть реалізовуватися разом. За допомогою Q-аналізу описані структурні залежності між уразливими місцями, що дозволяє отримати більш точну оцінку збитків.

11. Полуциганова В. І., Смирнов С. А. Оцінка ризиків в кібербезпеці за допомогою Q-аналізу. *XXI Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики»*: Всеукр. науково-практ. конференція студентів, аспірантів та молодих вчен., м. Київ, 12–13 трав. 2023 р. Київ, 2017. С. 172–173.

У роботі здобувачем розглянуто модель оцінки кібернетичного ризику з урахуванням зв'язків високих порядків та моделювання системи за допомогою Q-аналізу.

12. Polutsyhanova V. I., Smirnov S. A. Assessing cybersecurity risk with Q-analysis. *Всеукраїнська науково-практична конференція «Theoretical and Applied Cybersecurity» (TACS-2023)*, Kyiv, 26 May 2023. P. 57–60.

У роботі здобувачем представлено метод удосконалення оцінювання кібернетичного ризику з урахуванням зв'язків між уразливостями та загрозами на основі моделювання кіберсистеми за допомогою Q-аналізу.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

API – Application Programming Interface

BIOS – Basic Input/Output System

CRAMM – CCTA Risk Analysis and Management Method

CSA – Cloud Security Alliance

CVE – Common Vulnerabilities and Exposures

CVSS – Common Vulnerability Scoring System

CWE - Common Weakness Enumeration

DB – Data Breaches

IAM – Weak Identity, Credential and Access Management

IAM – Identity and Access Management

IDS – Intrusion Detection System

IDS – Intrusion Detection System (система виявлення вторгнень)

IoT – Internet of Things

MFC – Microsoft Foundation Classes

MTTSF – Time To System Failure

OCTAVE – The Operationally Critical Threat, Asset, and Vulnerability EvaluationSM

PRISM - Product Safety Risk Assessment Methodology

SC – Simplicial complex

SMM – Social Media Marketing

SQL – Structured Query Language

XML – Extensible Markup Language

БД – база даних

ІКІ – інформаційна критична інфраструктура

ІКС – інформаційно-комунікаційні системи

ІР – інформаційні ресурси

ІСОКІ – інформаційна система об’єкта критичної інфраструктури

НКЦК – Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України

СЗІ – системи захисту інформації

ВСТУП

Актуальність роботи

Аналіз оцінки ризиків через уразливості складних систем набуває все більшого значення для забезпечення їх безпеки. На сьогодні цей підхід є актуальним, адже поширення та вплив кіберсистем збільшується в усіх сферах життя, так чи інакше пов’язаних з інформаційними технологіями. У свою чергу, сучасний підхід щодо оцінювання ризиків у недостатній мірі ураховує специфіку інформаційної структури системи, а тому розрахунок оцінки ризиків є недостатньо точним та вимагає корегування.

Складний зв’язок між уразливими місцями системи обумовлений потенційними загрозами, які загострюються через їх присутність. Дисертаційне дослідження представляє моделі та методи виявлення, аналізу та класифікації загроз залежно від уразливостей, які притаманні системі. На основі проведеного аналізу структури сумісності вразливостей запропоновано метод оцінювання ризику з урахуванням специфіки взаємозв’язку вразливостей та загроз інформаційної системи. Цей підхід дозволяє краще усвідомити зв’язки між уразливими місцями кіберсистем, а також ступінь впливу на систему кожної з них окремо та спільно.

Найпоширенішим припущенням є те, що всі вразливості є незалежними та реалізуються внаслідок або випадкових подій, або зловмисних намірів. У роботі запропоновано метод, який дозволяє моделювати вразливості складних систем в цілому, з урахуванням їх прихованих зв'язків. Методи Q-аналізу використано для дослідження структури системи взаємопов’язаних уразливостей, які виникають у процесі реалізації загроз. Наведено приклад застосування методів Q-аналізу для синтезу оцінки ризику та запропоновано пояснення природи та впливу деяких потенційних загроз та їх комбінацій.

Оцінювання ризиків при реалізації загроз кіберінцидентів є основою для створення систем захисту кіберсистем. Запропонований метод включає урахування впливу структурних особливостей у взаємозалежності між

вразливостями та загрозами та допомагає точніше оцінити рівень ризику та зрозуміти його природу та характер, є актуальним.

Мета і задачі наукового дослідження. Метою дисертаційної роботи є розв'язання актуальної наукової задачі аналізу та синтезу моделей і методів оцінювання ризиків з врахуванням структурних властивостей сукупності зв'язків загроз та вразливостей кіберсистем, що дозволяє розробити процедуру побудови формули байєсівської оцінки ризику, виконати її аналіз та забезпечити уточнення оцінки ризику внаслідок врахування структури сумісності вразливостей системи.

Для досягнення поставленої мети необхідно розв'язати такі завдання:

1. Проаналізувати зв'язки між загрозами та вразливостями в сучасних кіберсистемах.
2. Дослідити ступінь наукової розробленості сучасних методів структурного аналізу складних систем.
3. Побудувати структурну модель сумісної реалізації та систему класифікації вразливостей та загроз для кіберсистем.
4. Розробити алгоритми для побудови структурних характеристик аналізу системи вразливостей та загроз.
5. Структурувати інформацію про загрози та вразливості кіберсистеми.
6. Розробити метод оцінювання ризику на основі врахування структурних особливостей системи та складених функцій втрат.
7. Проаналізувати можливості практичного використання розробленої методики.

Об'єкт: загрози і вразливості у складних кіберсистемах.

Предмет: оцінювання ризиків у складних кіберсистемах.

Для реалізації поставлених завдань у роботі були застосовані такі загальновідомі **методи:** методи теорії ймовірностей та математичної статистики, аналізу оцінки ризиків, прийняття рішень, Q-аналізу структури

симлеціальних комплексів, обчислень на графах, дослідження їх топології тощо.

У ході дослідження використовувалась мова програмування Python.

Дослідженню проблем, пов’язаних із розробкою методології оцінювання ризиків безпеки кіберсистем, таких як критичні інфраструктури, хмарні сховища тощо, присвячується значна частина публікацій вітчизняних та зарубіжних вчених, серед них: Архіпов О.Є., Аткін Р. Х., Грайворонський М. В., Джонсон Д. Х., Касті Д. Л., Качинський А. Б., Ланде Д. В., Мохор В. В., Новіков О. М. та інші науковці.

Однак, незважаючи на існуючі підходи щодо аналізу структури зв’язків уразливостей у кіберсистемах, запропонований у дослідженні метод оцінки ризику є актуальним.

Наукова новизна одержаних результатів полягає в обґрунтуванні теоретичних положень та розробленні практичних рекомендацій з удосконалення безпеки складноструктурних кіберсистем. На основі проведеного дослідження сформульовано нові положення та висновки, а саме:

- Вперше побудовано модель зв’язків загроз та вразливостей у кіберсистемі у вигляді симплеціального комплексу, яка представляє складну структуру їх взаємозалежностей, для класифікації загроз і вразливостей та для оцінювання потенційних втрат і ризиків;
- Вперше розроблено алгоритми аналізу симплекційного комплексу та його синтезу на основі повного набору структурних характеристик комплексу;
- Вперше розроблено метод класифікації загроз та вразливостей у складній системі з урахуванням характеристик власної розмірності підсистем, їх примикання та наслідування, що дозволяє надійніше оцінювати ризики в кіберсистемі в залежності від варіантів атак;
- Розроблено процедуру побудови байєсівської оцінки ризику з врахуванням структури вразливостей системи та складеної функції втрат.

Обґрунтованість і достовірність наукових результатів забезпечується коректним застосуванням математичного апарату та відповідних обчислювальних експериментів із використанням сучасного програмного забезпечення.

Практичне значення отриманих результатів.

Результати дослідження впроваджено у навчальний процес навчально-наукового фізико-технічного інституту НТУУ «КПІ імені Ігоря Сікорського», що підтверджено довідкою про впровадження в додатку Б.

Моделі та методи розроблені в дисертації використані в Науково-дослідні роботі «Підтримка прийняття рішень в умовах невизначеності та конкурентної взаємодії» номер державної реєстрації 0124U001957, що підтверджує наукову та практичну цінність отриманих результатів дослідження.

Наукові напрацювання та пропозиції даного дослідження використані під час підготовки матеріалів до засідання Ради національної безпеки і оборони України з питання «Про стан справ у енергетичній сфері», рішення Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України (далі – НКЦК), а також у процесі розроблення Загальних правил обміну інформацією про кіберінциденти, затверджених рішенням НКЦК (акт впровадження результатів дисертаційного дослідження наведено в додатку Б).

Отримані в дисертаційній роботі результати можуть бути застосовані в різних областях діяльності для розрахунку оцінки ризику в системах складної структури, передусім у кіберсистемах, на основі аналізу взаємозв’язків між уразливостями та загрозами. Застосування методу продемонстровано на практичному прикладі об’єкту інформаційної критичної інфраструктури.

Всі теоретичні і практичні результати дисертаційної роботи у повній мірі висвітлено у статтях, опублікованих у фахових вітчизняних наукових виданнях, що входять до відповідного встановленого переліку; виконано їх

належну апробацію на міжнародних та всеукраїнських наукових конференціях.

Особистий внесок здобувача. Основні положення і результати дисертаційної роботи, що виноситься до захисту, отримані автором самостійно. Дві фахові публікацій написані автором дисертації одноосібно, 2 фахові публікації – у співавторстві. Належна апробація результатів була проведена на конференціях та наведена в 8 тезах конференцій.

Здобувачеві належать такі результати:

У роботі [1] здобувачем введено такі поняття, як структурне дерево, локальні карти та процедура наслідування, які дозволяють роз'яснити зміст показників інформаційної системи, отриманих за допомогою Q-аналізу. На цій основі розроблено алгоритми для визначення основних метрик, які застосовано до банківської системи.

У роботі [2] здобувачем розроблено алгоритм відновлення або синтезу симлеціальних комплексів з елементарного набору симплексів за допомогою локальних бінарних карт і структурного дерева. Цей алгоритм використовується для зменшення збережених даних про систему, якщо комплекс описує велику складну систему, як-от систему кібербезпеки.

У роботі [3] здобувачем запропоновано метод, який дозволяє моделювати вразливості складних систем в цілому з урахуванням їх прихованих зв'язків. Q-аналіз використовувався для дослідження структури системи взаємопов'язаних уразливостей, які виникають у процесі реалізації проекту. Наведено приклад застосування методів Q-аналізу та запропоновано пояснення природного стану системи та впливу деяких потенційних загроз та їх комбінацій.

У роботі [4] здобувачем представлено методологію та приклад побудови, аналізу та класифікації вразливостей залежно від загроз, які вони породжують. Такий підхід висвітлює зв'язки та сумісну реалізацію між уразливими місцями, а також ступінь впливу кожної з них.

Апробація результатів дисертації. Результати та основні положення роботи подавалися та обговорювалися на:

1. Полуциганова В. І., Смирнов С. А. Використання q-аналізу для дослідження зв'язків у банківських системах. *XV Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики»*: Всеукр. науково-практ. конференція студентів, аспірантів та молодих вчен., м. Київ, 25-27 трав. 2017 р. Київ, 2017. С. 44-46.

2. Полуциганова В. І., Смирнов С. А. Використання алгоритмів q-аналізу на прикладі банківської системи. *XVI Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики»*: Всеукр. науково-практ. конференція студентів, аспірантів та молодих вчен., м. Київ, 26-27 квіт. 2018 р. Київ, 2018. С. 33-36.

3. Polutsyhanova V. The inverse problem of q-analysis. *XVIII Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики»:* Всеукр. науково-практ. конференція студентів, аспірантів та молодих вчен., м. Київ, 12-13 трав. 2020 р. С. 113-115.

4. Полуциганова В. І., Смирнов С. А. The inverse problem of Q-analysis of complex systems structure. *Інформаційні технології та безпека матеріали XXII міжнародної науково-практичної конференції* , м. Київ, 2021. С. 114–118.

5. Полуциганова В. І., Смирнов С. А. Оцінювання ризиків складних систем з використання методів Q-аналізу. *Інформаційні технології та безпека матеріали XXIII міжнародної науково-практичної конференції*, м. Київ, 2022. С. 51-52.

6. Полуциганова В. І., Смирнов С. А. Structure of vulnerability in complex systems and risk assessment// Міжнародна науково-практична

конференція «Виклики і загрози для критичної інфраструктури» 21-22 березня 2023 р. м. Київ, Україна. С. 334-335.

7. Полуциганова В. І., Смирнов С. А. Оцінка ризиків в кібербезпеці за допомогою Q-аналізу. *XXI Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики»*: Всеукр. науково-практ. конференція студентів, аспірантів та молодих вчен., м. Київ, 12-13 трав. 2023 р. м. Київ, 2017. С. 172-173.

8. Polutsyhanova V. I., Smirnov S. A. Assessing cybersecurity risk with Q-analysis. *Всеукраїнська науково-практична конференція «Theoretical and Applied Cybersecurity» (TACS-2023)*, м. Kyiv, 26 May 2023. P. 57-60.

Публікації. За матеріалами дисертації опубліковано 12 робіт, 4 з яких – статті у журналах і збірниках наукових праць, що входять до переліку фахових видань, затверджених МОН України за спеціальністю дисертації або у періодичних виданнях іноземних держав та 8 тез науково-практичних конференцій.

Структура та обсяг дисертації. Дисертація складається із анотації, вступу, чотирьох розділів, висновків, списку використаних джерел. Робота містить 207 сторінок, у тому числі: 186 сторінок основного тексту, 40 рисунків, 13 таблиць, списку використаних джерел із 109 найменувань на 12 сторінках, 2 додатків.

РОЗДІЛ 1

АКТУАЛЬНІСТЬ ПРОБЛЕМИ ОЦІНЮВАННЯ РИЗИКІВ ТА ЗАГАЛЬНІ ПІДХОДИ ДО ЇЇ РОЗВ'ЯЗАННЯ

1.1 Поточний стан методології оцінювання ризиків

На сучасному етапі розвитку людства відбуваються значні зміни пов'язані з запровадженням інформаційних технологій у різні сфери діяльності. Застосування таких технологій зумовлює використання інформаційних та кіберсистем, що призводить до ефективності обробки даних та інформації, але збільшує ризики пов'язаних із застосуванням та вразливостями таких систем. Необхідність оцінювати кіберризики стимулює розвиток методів, що враховують особливості кіберсистем.

Протягом останніх років застосування методів та підходів оцінювання ризику значно поширюється. Збільшується кількість нормативно-правових актів і стандартів, що приймаються, і які, у свою чергу, містять положення про оцінку ризику, а також вимагають застосування таких методів у різних сферах. Це сприяє розробці та удосконаленню відповідних методологічних підходів. Ураховуючи вищенаведене, цей тренд буде актуальним і надалі. [76].

Основна мета будь-якої оцінки ризику – забезпечити підтримку прийняття рішень. Коли приймається рішення, яке впливає на ризик, оцінка ризику допомагає, у тому числі усвідомити джерела ризику.

Використання методу оцінки ризику дозволяє вирішувати широке коло проблем від більш глобальних, таких як розташування виробничих потужностей – до технічних деталей того, як окрема система повинна функціонувати, і від суто технічних питань до проблем, пов'язаних із людськими та організаційними факторами.

Діапазон галузей (сфер) застосування методології оцінки ризиків, постійно розширюється. Деякі приклади найбільш поширених сфер застосування методів оцінки ризиків наведено в таблиці 1.1.

Таблиця 1.1 – Сфери застосування методів оцінки ризику для проведення аналізу

Сфера застосування методів оцінки ризику	**Напрямки застосування або проблемна зона**
Небезпечні речовини	Хімічна/переробна промисловість, нафтова промисловість (включаючи трубопроводи), промисловість вибухових речовин, атомна промисловість
Транспорт	Повітряний рух (літаки, вертольоти, дрони), залізниця, морський транспорт, автомобільний транспорт
Космічна галузь	Космічна техніка та проекти
Безпека продукції	Технічні продукти, такі як машини, автомобілі, роботи, автономні системи
Критичні інфраструктури	Питне водопостачання, каналізаційні системи, електромережі, системи зв'язку, лікарні та охорона здоров'я, банківська справа і фінансові системи
Медичний сектор	Медичне обладнання, роботизовано хірургія, бактерії/віруси
Робота, діяльність	Промисловість, сільське господарство, лісове господарство, спорт

Захист навколишнього середовища	Забруднюючі речовини, CO_2, підвищення загальної температури, підвищення рівня океану
Безпека харчових продуктів	Зараження, інфекція
Безпека для здоров'я	Тютюн, алкоголь, радіація, ракові клітини
Проектний ризик	Час і вартість великих проектів (наприклад, будівництво, програмне забезпечення)
Економічний/фінансовий	Страхування, інвестиційні, фінансові, підприємницькі та проектні ризики
Кібербезпека	Диверсії, крадіжки, кібератаки, шпигунство, тероризм

Дослідженню проблем, пов’язаних із розробкою методів оцінювання ризиків безпеки складних кіберсистем, таких як критичні інфраструктури, хмарні сховища тощо, присвячується значна частина публікацій вітчизняних та зарубіжних вчених, серед них: Архіпов О.Є., Аткін Р. Х., Грайворонський М. В., Джонсон Д. Х., Касті Д. Л., Качинський А. Б., Ланде Д. В., Мохор В. В., Новіков О. М. та інші науковців. У наступних підрозділах більш детально розглянуто теоретичну базу структурного аналізу кіберсистем, методів оцінювання ризиків, методології управління вразливостями кіберсистем.

1.1.1 Пріоритизація ризиків

Для визначення пріоритету ризику часто застосовується такий проектний індикатор, як показник важливості ризику (risk exposure). Але недоліком цього показника є те, що він дає ідентичний результат як для

високої ймовірності й низького рівня втрат (high-probability/low-impact), так і для низької ймовірності й високого рівня втрат (high-impact/low-probability). Ураховуючи вищенаведене, кращим способом оцінювання ризиків є матриця ризиків.

Матриця ризиків є інструментом для оцінювання пріоритетності ризиків. Комбінуючи два показники (ймовірність і втрати) для обчислення важливості ризику, отримуємо можливість прийняти більш ефективне рішення про те, які з множини можливих ризиків заслуговують на подальшу увагу.

Зазвичай кожна організація самостійно встановлює рівень поєднання імовірності події та її вплив на систему, на основі яких ступінь ризику визначається як «високий», «середній» або «низький». Це, зі свого боку, визначає пріоритетність при плануванні комплексу заходів для реагування на кожен ризик. Поєднання імовірності події та її вплив на систему в процесі планування управління ризиками може переглядатися і адаптуватися до кожного проекту. На основі цього та аналогічних розподілів для загроз проекту від наслідків дії ризику будується матриця ризиків (таблиця 1.2).

Таблиця 1.2 – Матриця ризиків

Ймовірність	**Наслідок**		
	Низький=1	**Середній=2**	**Високий=3**
Висока=3	3	6	9
Середня=2	2	4	6
Низька=1	1	2	3

Важливість ризику, наведена у таблиці, має такі якісні характеристики:

1 – 2 – низький ризик;

3 – 4 – середній ризик;

6 – 9 – високий ризик.

Коли у відповідні клітинки матриці вписуються ризики, які ідентифіковані й виміряні, вигляд матриці буде таким як, наведено у таблиця 1.3.Таблиця 1.3 – Матриця ризиків

Рівень ризику				
Ймовірність	**Великий**		ризик 10	ризик 2
	Середній		ризик 1	ризик 3
	Малий	ризик 4 ризик 5 ризик 8	ризик 9	ризик 6 ризик 7
		Малий	**Середній**	**Великий**
		Вплив		

У матриці ризиків розміщують ймовірність і наслідок ризику в двовимірному просторі. Це дає декілька переваг:

1. Ризики високої ймовірності та низького рівня втрат (highprobability/low-impact) й низької ймовірності та високого рівня втрат (high-impact/low-probability) розрізняються.

2. Ризики можна візуально порівняти.

3. Ступінь пріоритетності ризиків визначається в матриці, в якій зверху справа розміщаються ризики високої ймовірності та пріоритетності, а зліва знизу – малоймовірні ризики з низьким рівнем втрат (low-probability/low-impact).

У таблиці ризиків часто для візуалізації пріоритетів ризиків використовуються жовтий, червоний та білий кольори (рисунок 1.1).

Кольорова візуалізація полегшує команді управління ризиками підібрати відповідні заходи:

– готувати повний план реагування для кожного елементу таблиці з високим ризиком (ці ризики відслідковуються дуже ретельно);

– створювати план реагування для тих елементів середнього ризику, для яких це необхідно;

– для елементів низького ризику ніякого реагування не передбачається [80].

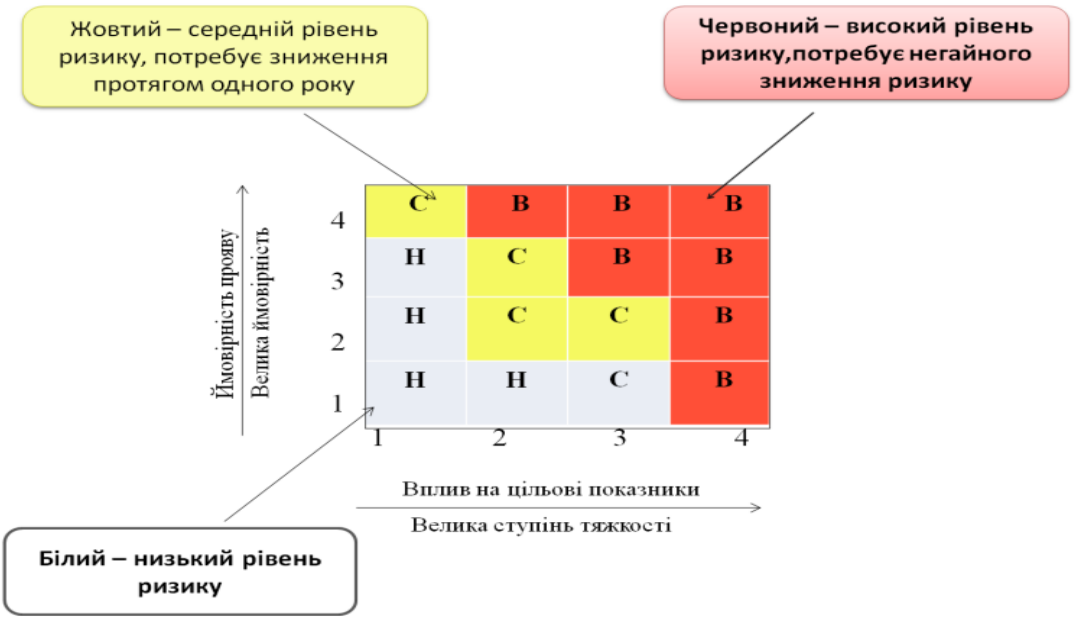


Рисунок 1.1 – Таблиця ризику з кольорами візуалізації пріоритетів ризиків [80]

Деякі математичні питання властивості матриць ризиків наведено у роботі [76] і показано їх обмеження.

• Погана роздільна здатність. Типові матриці ризиків можуть правильно й однозначно порівнювати лише невелику частку (наприклад, менше 10 %) випадково вибраних пар небезпек. Вони можуть призначити однаковий рейтинг кількісно відмінним ризикам («стиснення обсягу»).

• Порівняння помилок в оцінках. Матриці ризиків можуть неправильно призначати вищі якісні оцінки нижчим кількісним ризикам. Для ризиків, де частота та серйозність наслідків мають від'ємну кореляцію, і при цьому вони можуть бути «гіршими, ніж неважливими». Це призводить до того, що випадкове прийняття рішень може бути кращим за наведені результати.

• Неоптимальний розподіл ресурсів. Ефективний розподіл ресурсів для контрзаходів, спрямованих на зниження ризику, часто не може базуватися на категоріях, наданих матрицею ризиків.

• Неоднозначні входи та виходи. Для непереконливих результатів категорії відносної тяжкості наслідків не обов'язково є об'єктивними (незалежно від суб'єктивного ставлення до ризику). Вхідні дані (наприклад, класифікація частоти та тяжкості наслідків) та вихідні дані (тобто оцінки ризику) матриці ризику вимагають суб'єктивної інтерпретації. Різні користувачі можуть отримати протилежні оцінки того самого кількісного ризику. Ці обмеження свідчать про те, що, навіть якщо матриці ризику необхідні, їх слід використовувати з обережністю та лише з ретельною інтерпретацією включених оцінок.

Оцінка ризику повинна надати більш об'єктивну інформацію, яка у кінцевому підсумку дозволить знайти баланс між використанням можливостей отримання прибутку та мінімізацією негативних наслідків. Це ітеративний пошук, який в ідеальному випадку веде до постійного вдосконалення процесу прийняття рішень, і сприяє постійному зростанню ефективності [100].

Ризик також стосується системи оцінювання якості. Впровадження системи якості має забезпечувати можливість використання різних джерел і методів для отримання результатів певного рівня, тобто таких, що відповідатимуть потребам користувачів. Як і ризик, рівень якості можна визначити з інституційного середовища та цілей конкретної установи. У цьому випадку інституційне середовище визначає загальний рівень ризику, який організація готова прийняти для досягнення своїх цілей.

Процес оцінки та управління ризиками можна розділити на кілька етапів: визначення структури, ідентифікація ризиків, аналіз ймовірності та впливу ризиків, оцінка ризиків і, нарешті, реагування на ризики.

Першим кроком є визначення стратегічних, організаційних та управлінських ризиків, які є основою для всього подальшого процесу. Це включає встановлення критеріїв оцінки ризику та визначення структури аналізу.

Другим кроком є визначення подій, які можуть вплинути на досягнення цілей. Ідентифікація повинна містити запитання про тип ризику, час і місце

події, а також те, як подія запобігла, порушила, затримала або прискорила досягнення цілей.

Наступним кроком є визначення існуючих засобів контролю та аналіз ризиків з точки зору ймовірності та потенційних наслідків. Основні підходи в оцінюванні ризику такі, як графічний та аналітичний, описані в [102-103].

Оцінений рівень ризику можна порівняти зі заздалегідь визначеними критеріями, щоб визначити баланс між потенційними перевагами та негативними наслідками.

Останнім кроком є визначення того, як вплинути на ризик. Ризики нижче певного рівня можна ігнорувати або не впливати на них. З іншого боку, витрати на пом'якшення ризиків можуть бути занадто високими та перевищувати потенційні вигоди. У таких випадках організація може прийняти рішення припинити свою діяльність. Ризики також можна передати третім сторонам, наприклад, через страхування, щоб компенсувати витрати. Останнім варіантом є розгляд ризиків, пов'язаних із стратегією чи дією, та порівняння витрат із потенційними вигодами. У цьому випадку організація вирішує, яким чином реалізувати стратегію для максимізації вигод і мінімізації потенційних втрат.

Наприклад, фактори, які слід ураховувати при вимірі якості «установа/бізнес-середовище», включають стабільність постачальника даних. Існує відповідний ризик того, що постачальник даних не зможе надавати дані в майбутньому. Інший приклад стосується запропонованого параметра якості «конфіденційність і безпека». Одним із ключових елементів є «сприйняття», яке стосується ймовірності того, що різні зацікавлені сторони матимуть негативне сприйняття передбачуваного використання певного джерела даних [87-89].

1.1.2 Типізація ризиків

Поява поняття «мережевий ризик» є першим кроком для підприємств, щоб зрозуміти важливість безпеки мережі. «Кіберризик» відноситься до

ризику фінансових втрат (прямих і непрямих), припинення діяльності або її скорочення, а також шкоди для репутації організації або особи. Часто це визначення супроводжується чимось на зразок: «через порушення роботи інформаційних служб і систем». Поняття кібербезпеки набагато ширше, ніж поняття інформаційні системи та поняття інформаційні ресурси. Воно охоплює всі ресурси компанії або організації, включаючи співробітників, підрядників і партнерів. Будь-яка сфера діяльності або діяльність, яка може спричинити загрозу реалізації вищезазначених ризиків, становить систему покриття кіберризиків.

Управління кіберризиками є основою будь-якої операції з безпеки, чи то впровадження систем або інструментів, створення процесів і впровадження правил і політик. Програми управління ризиками часто недооцінюють. Хоча, саме ефективне визначення та управління кіберризиками дозволяє раціонально розподілити бюджет на кібербезпеку та заздалегідь підготуватися до атак і загроз.

Існує кілька передумов, наведених нижче, для формалізації процесу управління кіберризиками.

Цифровізація (або «диджиталізація») сучасного бізнесу. Практично кожна галузь включає кіберпростір, і розмір компанії більше не має значення.

Фахівці вже є інформаційним активом, який необхідно захищати. Дозвольте фахівцям самостійно зрозуміти масштаби використання кіберризику. Сфера безпеки стає все більш взаємозалежною. Наприклад, фізична безпека для IoT. Найвищому керівництву потрібен простий для розуміння інструмент для оцінки безпеки системи та її розвитку.

У світі існує багато методів структурування процесу управління ризиками та початкової оцінки ризиків. Coras, CRAMM, PRISM, RiskWatch, OCTAVE – лише деякі з переліку існуючих практичних методів. Є загальний підхід і є розгалужений. Для досвідченого консультанта не складно створити процес оцінки та управління кіберризиками за допомогою будь-якого з них [97].

Для компаній, які ніколи раніше не займалися ризик-менеджментом, і не знають, що таке матриця ризиків і для чого вона необхідна, варто почати з аналізу ризиків. Навіть якщо процес управління ризиками буде впроваджено та встановлено, здійснення аналізу ризиків буде залишатися актуальним, оскільки кіберризики є дуже динамічною субстанцією, і вони часто сильно змінюються. Під час початкового процесу оцінки ризиків спочатку необхідно визначити цілі компанії щодо управління кібербезпекою.

Після цього необхідно визначити ключові елементи, які впливають на ключові бізнес-процеси компанії. У класичному розумінні кожен ризик оцінюється за двома параметрами: ймовірність і потенційні втрати. На основі цих кількісних показників формується карта ризиків та їх пріоритетів. Такі оцінки необхідно проводити постійно, розширюючи карту ризиків, щоб охопити якомога більше потенційних ризиків компанії.

Наступним кроком є визначення бізнес-пріоритетів на основі оцінки кіберризиків. Загалом, це фінансовий показник, зрозумілий топ-менеджменту та представникам бізнес-підрозділів [105].

Потім починається робота з ризиком. Необхідно проаналізувати кожен ризик після оцінки, щоб сформулювати контрзаходи. Існує класичний набір таких заходів: мінімізувати, прийняти, уникати, відвернути та диверсифікувати. Однак нові терміни чи інструменти можуть з’являтися разом з іншими техніками.

Завдання цієї фази роботи полягає у виборі правильного інструменту управління для кожного ризику (який можна переглянути та змінити пізніше). Наприклад, іноді компанії ризикують втратити клієнта, оскільки розуміють, що боротися за нього економічно невигідно. Таким чином, у сфері кібербезпеки захист певних ресурсів або активів може бути недоцільним тому, що їх втрату або пошкодження легше прийняти.

Наступним кроком є застосування вибраних інструментів і заходів управління кіберризиками та перевірка їх ефективності. У рамках наступного перегляду матриці ризиків цілком може виявитися, що обраний підхід до

управління ризиками не виправдав очікувань, що ризик змінив свої параметри (ймовірність і збитки), які вимагають більш жорстких або, навпаки, м’яких заходів і, відповідно, є більш або менш затратними.

Останнім кроком є переоцінка, а точніше, періодичний перегляд карт процесів і мережевих ризиків. Цей підхід допомагає врахувати актуальну інформацію та усунути поточні загрози. Унаслідок компанія підтримує найвищий рівень кіберстійкості, відслідковуючи пріоритети ризиків та ефективно керуючи ними. Кіберзагрози не припиняться, а атаки не зменшаються, тому превентивна оцінка та підготовка до найбільш небезпечних подій залишається вірним і необхідним кроком у сучасному світі [77, 81-84].

1.2 Загальні підходи до оцінювання ризику

Оцінювання кіберризику тісно пов’язано з прийняттям рішень. Цей процес обумовлений подіями, які відбуваються в самій системі, та маніпуляціями над нею. Для моделювання цих подій найчастіше використовують методи з теорії ймовірності та випадкових процесів.

Спочатку проілюструємо рішення, запропоновані в галузі класичної теорії прийняття рішень, яка має справу з проблемами прийняття рішення в умовах невизначеності, тобто коли попередні ймовірності, а також будь-який інший тип інформації про природний стан системи недоступні або значно обмежені. Проаналізуємо критерії прийняття рішень з огляду на збитки, а не грошові еквіваленти.

Відтак, у тексті використовується типова позиція, для ілюстрації основ класичної статистичної теорії прийняття рішень, у якій вибіркова інформація надається особі, яка приймає рішення, щоб покращити його/її знання про стан середовища, навіть якщо попередньої інформації немає.

Введемо поняття функції рішення та ризику (очікуваних втрат). Показано, що вибіркову інформацію можна використовувати для обчислення ризику, пов’язаного з відповідною функцією прийняття рішення та природним

станом системи. Наведемо типовий підхід для байєсової статистичної теорії прийняття рішень, яка має справу з ситуаціями прийняття рішень, коли доступна як вибіркова, так і попередня інформація. У цьому контексті вводяться поняття очікуваного ризику та апостеріорної ймовірності, а також ілюструється еквівалентність між звичайною та розширеною формами аналізу рішень. Традиційні проблеми статистичного висновку (тобто оцінка та перевірка гіпотез) суперечать перспективі прийняття рішень у класичній та байєсовій теоріях прийняття рішень.

Що стосується отримання вибіркової інформації, то витрати, пов'язані з вибіркою, також обговорюються та формалізуються в процесі прийняття рішень: очікувана вартість досконалої інформації, очікувана вартість вибіркової інформації та концепція чистого прибутку, пов'язана з вибіркою [56].

Щоб забезпечити концептуальну основу, пов'язану з темами, розглянутими в наступних розділах, підсумовуємо основні моделі, які застосовуються у процесі прийняття рішень:

– імовірнісна модель *f(x;Θ)*, що враховує спільний розподіл вибіркових спостережень і природного стану;

– простір станів (або простір параметрів) Θ, який у багатьох випадках має розмірність R_k і може бути дискретним або неперервним;

– дискретний простір дій A =($a_1, a_2, ...$);

– дискретний простір *E* експерименту;

– простір вибірки *Ω*, що складається з результатів кожного експерименту (для однофакторної випадкової змінної результати вибірки виражаються як n (розмір вибірки) дійсних чисел);

– дискретний простір розв'язків D = ($d_1, d_2, ...$).

Крім того, представлено такі функції:

– функція корисності U = u(a_i; Θ_j) = u_{ij}, яка пов'язує результати, виражені в корисності, з кожною дією та природним станом системи;

– функція втрат l_{ij} = l(a_i; Θ_j) = - u(a_i; Θ_j), яка пов'язує результат, виражений у втратах, із кожною дією та природним станом системи;

– функція прийняття рішення d_h = δ_h(x), яка відображає кожну точку в просторі Ω, вибірки в простір дії A^1.

1.2.1 Оцінка ризику в підході Вальда

Зі статистичної точки зору поняття функції корисності часто замінюють поняттям додаткової функції втрат l_{ij}, яка розраховується за формулою (1.1) [56].

$$l_{ij} = l(a_i; \Theta_j) = - u(a_i; \Theta_j), \quad (1.1)$$

Теорія статистичних рішень розглядається в термінах вихідної установки, наданої Абрахамом Вальдом [58], що відповідає типовому статистичному висновку. Ця тема також широко обговорюється Фергюсоном Т. С. [59], Де Гротом М. Х. [60], Бергером Д. О. [61], Людовиком Пічінато [62] і Робертом К. П. [63]. Нижче посилаємося на традиційні інструменти статистичного висновку, а саме на точкову оцінку та перевірку гіпотез.

Найкращою оцінкою є ефективність, яка традиційно вимірюється в термінах середньої простої помилки або середньої квадратичної помилки. Середня проста помилка або середньоквадратична помилка розраховується за допомогою функції втрат l_{ij}, де a_i представляє оцінку $\hat{\Theta}$, а Θ_j представляє справжнє значення невідомого параметра.

Ураховуючи вищенаведене проблема прийняття рішення «вибір оптимальної оцінки $\hat{\Theta}^*$» вирішується шляхом пошуку найбільш ефективної оцінки, тобто оцінки, яка мінімізує середню просту помилку:

$$\hat{\Theta}^* = \arg\left[\min_{\theta\in\mathbf{\Theta}} l(\hat{\Theta}^*, \theta)\right] = \arg\left[\min_{\theta\in\mathbf{\Theta}} mse(\hat{\Theta}^*)\right] = \arg\left[\min_{\theta\in\mathbf{\Theta}} E(|\hat{\Theta}^* - \quad (1.2)$$

або середньоквадратичну помилку:

$$\hat{\Theta}^* = \arg\left[\min_{\theta\in\mathbf{\Theta}} l(\hat{\Theta}^*, \theta)\right] = \arg\left[\min_{\theta\in\mathbf{\Theta}} MSE(\hat{\Theta}^*)\right] = \arg\left\{\min_{\theta\in\mathbf{\Theta}} E[(\hat{\Theta}^* - \theta)^2]\right\} \quad (1.3)$$

Так само, виходячи з теорії перевірки гіпотез, ми можемо інтерпретувати ймовірність помилки типу II як функцію втрат, яку необхідно мінімізувати, ураховуючи частоту помилок типу I.

Критерій рішення, уведений як функція (грошового) результату, тепер може бути виражений у термінах збитків.

Мінімально-максимальний критерій або критерій А. Вальда (надзвичайно песимістичний погляд) розраховується за формулою (1.4).

$$a^* = \arg\left[\min_i(\max_j\ l_{ij})\right] = \arg\left[\min_i(\max_j\ l(a_i,\theta_j))\right]; \tag{1.4}$$

Мін-мін критерії (надзвичайно оптимістичний погляд) розраховуються за формулою (1.5).

$$a^* = \arg\left[\min_i(\min_j\ l_{ij})\right] = \arg\left[\min_i(\min_j\ l(a_i,\theta_j))\right]; \tag{1.5}$$

Критерій Адольфа Гурвіца розраховується за формулою (1.6).

$$\begin{aligned} a^* &= \arg\left\{\min_i\left[(1-\alpha)\max_j\ l_{ij} + \alpha\min_j\ l_{ij}\right]\right\} \\ &= \arg\left\{\min_i\left[(1-\alpha)\max_j\ l(a_i,\theta_j) + \alpha\min_j\ l(a_i,\theta_j)\right]\right\}; \end{aligned} \tag{1.6}$$

Критерій Леонарда Севіджа або критерій мінімального-максимальної втрати розраховується за формулою (1.7).

$$a^* = \arg\left[\min_i(\max_j\ r_{ij})\right] \tag{1.7}$$

де $r_{ij} = l_{ij} - l_{ij} = l(a_i; \Theta_j) - l(a_i; \Theta_j)$.

Крім того, ці критерії можна виразити в термінах корисності: відмінність полягає в максимізації корисності, а не в мінімізації втрат, але результат той самий, більш конкретно.

Критерій max-min або критерій Абрахама Вальда (надзвичайно песимістичний погляд) розраховується за формулою (1.8) [58].

$$a^* = \arg\left[\max_i(\min_j\ u_{ij})\right] = \arg\left[\max_i(\min_j\ u(a_i,\theta_j))\right]; \tag{1.8}$$

Max-max (крайня оптимістична перспектива) розраховується за формулою (1.9).

$$a^* = \arg\left[\max_i(\max_j\ u_{ij})\right] = \arg\left[\max_i(\max_j\ u(a_i,\theta_j))\right]; \tag{1.9}$$

Критерій Гурвіца розраховується за формулою (1.10).

$$\begin{aligned} a^* &= \arg\left\{\max_i\left[(1-\alpha)\min_j\ u_{ij} + \alpha\max_j\ u_{ij}\right]\right\} \\ &= \arg\left\{\max_i\left[(1-\alpha)\min_j\ u(a_i,\theta_j) + \alpha\max_j\ u(a_i,\theta_j)\right]\right\}; \end{aligned} \tag{1.10}$$

Критерій Севіджа або мінімально-максимальний критерій втрати (визначення оптимальної дії з втратами, які тепер визначаються) розраховується за формулою (1.11).

$$r_{ij} = \max_i u_{ij} - u_{ij} = \max_i u(a_i,\theta_j) - u(a_i,\theta_j). \tag{1.11}$$

Як уже підкреслювалося, ці критерії прийняття рішень мають певний ступінь прийнятності (суб'єктивності): аргументи на користь вибору того чи іншого критерію залежать від обставин прийняття рішень, в яких хтось діє.

1.2.2 Статистичний підхід Байєса до оцінки ризику

У розглянутих вище прикладах припускалося, що особа, яка приймає рішення, має лише попередню інформацію про природні стани системи (байєсова теорія прийняття рішень), або що він/вона знаходиться в невизначеній ситуації без будь-якої інформації про природний стан системи, або може використовувати лише апріорну інформацію в розрахунках ризиків. Також зазначалося, що загалом неможливо визначити функцію прийняття рішень, що мінімізує ризик, для кожного окремого природного стану системи. Іншими словами, не існує домінуючого рішення.

Перший підхід полягає в застосуванні одного з критеріїв прийняття рішення в умовах невизначеності, беручи до уваги підмножину прийнятних (і розумних) функцій прийняття рішення. Другий підхід базується на формальному введенні розподілу ймовірностей природного стану. Це дає можливість розрахувати очікуване значення ризику та визначити рішення, яке мінімізує його (звичайна форма аналізу).

Альтернативний підхід, який веде до того самого результату, полягає у використанні додаткової вибіркової інформації шляхом застосування формули Т. Байєса (аналіз розширеної форми) для оновлення попередньої інформації, представленої розподілом ймовірностей природного стану. Слід підкреслити, що часто буває досить складно розглядати попередні ймовірності через байєсові формулювання. Це особливо вірно, якщо неможливо ідентифікувати статистику, розподіл якої однозначно визначається даними вибірки. З іншого боку, коли існує кілька природних станів системи і результатів вибірки, дуже важко або навіть неможливо визначити всі функції прийняття рішень.

Наявність зразкової інформації дозволяє розрахувати ризик або очікувані втрати для кожної функції прийняття рішення та кожного природного стану системи. Крім того, якщо також застосувати відомий розподіл ймовірностей природного стану системи, інформація про ризик може бути синтезована через очікуваний ризик, тобто очікуване значення очікуваного збитку.

Означення. Очікуваний ризик. Припускаємо, що є випадкова вибірка $x' = (x_1, x_2, \dots x_n)$, функція прийняття рішень $d_h = (x_1, x_2, \dots x_n) = \delta(x)$, кінцевий дискретний набір природних станів $\Theta = (\Theta_1, \Theta_2, \dots \Theta_n)$, (об'єктивна чи суб'єктивна) ймовірність $\pi(\theta_1), \dots \pi(\theta_n)$, тоді очікуваний ризик розраховується за формулою (1.12) [56]:

$$E_\theta[R(d_h, \theta_j)] = \sum_{j=1}^{k} R(d_h, \theta_j)\pi(\theta_j). \qquad (1.12)$$

Подібним способом, якщо набір станів Θ є неперервним, визначається очікуваний ризик за формулою (1.13).

$$R(d_h, \theta_j) = E_{\boldsymbol{x}}\{l[\delta_h(\boldsymbol{x}), \theta_j]\}, \tag{1.13}$$

Очікуваний ризик отримується шляхом обчислення подвійного математичного очікування значення функції втрат від результату вибірки та природного стану системи за формулою (1.14).

$$E_\theta[R(d_h, \theta_j)] = E_\theta E_{\boldsymbol{x}}\{l[\delta_h(\boldsymbol{x}), \theta_j]\}. \tag{1.14}$$

Заслуговують на увагу аналогії між концепцією очікуваного ризику та очікуваної корисності. Основна відмінність полягає в тому, що в очікуваному ризику враховуються втрати, а не корисність, і що результати вибірки враховуються наочно. Оптимальне рішення – це таке, яке мінімізує очікуваний ризик та розраховується за формулою (1.15).

$$\begin{aligned} d^* &= \arg\left\{\min_{d_h} E_\theta\left[R(d_h, \theta_j)\right]\right\} \\ &= \arg\left\{\min_{\delta_h}\left[E_\theta E_{\boldsymbol{x}}(l(\delta_h(\boldsymbol{x}), \theta_j))\right]\right\}. \end{aligned} \tag{1.15}$$

Якщо параметр станів Θ і простір вибірки Ω є неперервними, оптимальне рішення розраховується за формулою (1.16):

$$\begin{aligned} d^* &= \arg\left\{\min_{d_h}\left[E_\theta\left(R(d_h, \theta_j)\right)\right]\right\} \\ &= \arg\left\{\min_{d_h}\left[\sum_{j=1}^{k} R(d_h, \theta_j)\pi(\theta_j)\right]\right\} \\ &= \arg\left\{\min_{\delta_h}\left[\sum_{j=1}^{k}\left(\sum_{h=1}^{r} l(\delta_h(\boldsymbol{x}), \theta_j) f(\boldsymbol{x}|\theta_j)\right)\pi(\theta_j)\right]\right\}. \end{aligned} \tag{1.16}$$

Подібним способом, якщо параметричний простір і простір вибірки є неперервними, оптимальне рішення розраховується за формулою (1.17):

$$\begin{aligned} d^* &= \arg\left\{\min_{d_h}\left[E_\theta\left(R(d_h, \theta_j)\right)\right]\right\} \\ &= \arg\left\{\min_{d_h}\left[\int_\theta R(d_h, \theta)\pi(\theta)d\theta\right]\right\} \\ &= \arg\left\{\min_{\delta_h}\left[\int_\theta\left(\int_{\boldsymbol{x}} l(\delta_h(\boldsymbol{x}), \theta) f(\boldsymbol{x}|\theta)d\boldsymbol{x}\right)\pi(\theta)d\theta\right]\right\}. \end{aligned} \tag{1.17}$$

Добутки $f(x|\theta_j)\pi(\theta_j)$ та $f(x|\theta)\pi(\theta)$ з'являються в усіх наведених вище формулах. Ці формули показують, як вибіркова інформація сприяє оновленню попередньої інформації, таким чином забезпечуючи апостеріорний розподіл ймовірностей за станом класичної та байєсової теорії статистичних рішень (розширений формальний аналіз).

1.2.3 Метод ланцюгів Маркова в метриках безпеки для оцінювання ризиків

Розглянемо показники безпеки, пов'язані з розподілом ймовірностей загроз безпеці, наведених Н. Т. Ли й Д. Б. Хоангом [57]. А. Б. Аіссою запропоновано для використання показник безпеки під назвою «середня вартість відмови» (далі – MFC) [64]. Цей показник застосовується для вимірювання безпеки ІТ-систем шляхом кількісного визначення показників, включаючи зацікавлені сторони, втрати, спричинені загрозами безпеці [65]. Перевага цього показника полягає в тому, що він виконує кілька бажаних функцій: визначає зацікавлені сторони і надає кожній з них вартість через збій безпеки системи; вимірює вартість економічної шкоди за одиницю часу перевірки ($/год). Незважаючи на ці наведені вище переваги, MFC страждає від серйозних недоліків, оскільки розподіл ймовірностей загроз безпеці базується на простих емпіричних даних, тоді як загрози безпеці змінюються, оскільки є динамічними та специфічними для різних ІТ-систем. Унаслідок випадкового характеру загроз, моделювання їхнього розподілу ймовірностей призводить до необхідності вимірювання та прогнозування безпеки для будь-якої системи. Релевантна й надійна класифікація загроз на основі розгорнутих уразливостей, прогнозу мотивації атаки та ймовірності успішної атаки має вирішальне значення для полегшення ідентифікації потенційних загроз безпеці та формулюванню контрзаходів для забезпечення безпеки.

Для марковського процесу умовний розподіл ймовірностей майбутнього стану процесу (залежно від минулого та поточного станів) залежить лише від поточного стану, а не від послідовності подій, що йому передують.

Ґрунтуючись на цій властивості, в різних дослідженнях використовувалася марковська система для моделювання показників безпеки.

А. Бар та інші використовують дискретні ланцюгові моделі Маркова для прогнозування наступних атак [65]. У дослідженнях А. Патча та Д. Парка для виявлення аномальних атак у системах виявлення вторгнень (далі – IDS) система моделюється за допомогою прихованих ланцюгів Маркова [68]. С. Канчанапокін та С. Бункронг застосували напівмарковську модель (далі – SMM) для кількісної оцінки стану безпеки системи захисту від вторгнень. Вони застосували ймовірність сталого стану ланцюга Маркова з дискретним часом (далі – DTMC), щоб обчислити безпечний середній час до відмови (далі – MTTSF). С. Джафар та ін. концепцію шляху атаки та час використали для розрахунку ймовірностей переходу [66]. Що стосується показників безпеки, більшість досліджень використовують моделі Маркова для прогнозування атак на безпеку або поширення шкідливого програмного забезпечення.

Загрози безпеці розглядаються як потенційні атаки, які призводять до неправомірного використання інформації або ресурсів, тоді як уразливості визначаються як недоліки в кіберпросторі, якими можуть скористатися хакери. Таким чином, загроза безпеці – це потенційна атака, яка може відбутися або не відбутися, але потенційно може завдати шкоди.

Приклади загроз безпеці хмарним середовищам наведені у звіті Cloud Security Alliance (далі – CSA) [67]. У звіті описано 12 критичних загроз безпеці, які впливають на спільний доступ до хмарних обчислень на вимогу, та мають найбільший вплив на бізнес підприємства:

• Порушення даних (далі – DB).

• Незахищені інтерфейси (далі – API) (інтерфейс прикладного програмування).

• Уразливості системи (далі – SV).

• Викрадення облікового запису (далі – AH).

• Зловмисні інсайдери (далі – MI).

• Розширені стійкі загрози (далі – APT).

• Втрата даних (далі – DL).

• Недостатня належна перевірка (далі – IDD).

• Зловживання та нечесне використання хмарних служб (далі – ANU).

• Відмова в обслуговуванні (далі – DOS).

• Спільні технологічні вразливості (далі – STV).

Більш детально з описом загроз можна ознайомитись в [57].

Загроза безпеці зазвичай використовує одну або кілька вразливостей у компонентах системи для її компрометації. Таким чином, зв’язок між уразливими місцями безпеки та цими визнаними загрозами є важливим для моделі загроз.

К. Хашизуме та ін. [70] визначив сім основних уразливостей безпеки при проведенні обчислень у хмарних середовищах, а саме:

• Незахищені інтерфейси та API (V1).

• Необмежений розподіл ресурсів (V2).

• Уразливості, пов'язані з даними (V3).

• Уразливості у віртуальних машинах (V4).

• Уразливості в образах віртуальних машин (V5).

• Уразливості в гіпервізорах (V6).

• Уразливості у віртуальних мережах (V7).

Більш детально з описом уразливостей можна ознайомитись у публікації Ли Н. Т. й Хоанга Д. Б. [57]. Ними визначено та встановлено зв’язки між загрозами безпеці та вразливими місцями. З виокремлених зв’язків виплаває, загроза безпеці може мати кілька вразливостей, і одна вразливість може бути використана кількома загрозами безпеки. Наприклад, розглянемо загрозу порушення даних (DB). Ця загроза безпеці включає п’ять уразливостей: незахищений інтерфейс і API (V1), уразливість даних (V3), уразливість віртуальної машини (V4), уразливість зображення віртуальної машини (V5) і вразливість віртуальної мережі (V7).

Т. Рістенпат та ін. зазначив, що конфіденційну інформацію можна отримати з віртуальних машин, розташованих на одному сервері [71].

Зловмисники можуть використовувати вразливості методів обробки даних у хмарних системах під час підбору даних, вимірювання, використання кешу та виявлення зв'язків між елементами системи на основі навантаження, щоб збирати дані за допомогою кількох атак.

Таким чином, порушення даних залежать не лише від уразливостей, пов'язаних із даними, але й від уразливостей віртуалізації.

Як видно з таблиці [57], ця вразливість даних (V3) містить три загрози безпеці. По-перше, коли зловмисники використовують різні методи, такі як впровадження SQL і міжсайтовий сценарій для атаки на хмарні системи, це може спричинити загрози витоку даних (далі – БД). По-друге, такі дії можуть призвести до слабких ідентифікаційних даних, облікових даних і загроз керування доступом (далі –IAM). Зловмисники можуть отримати доступ до хмарних систем, використовуючи дані, які часто зберігаються, обробляються та передаються публічно. По-третє, загрози втрати даних (DL) можуть виникнути, коли зловмисники використовують численні вразливості, такі як дані в різних місцях, неповне видалення даних і резервне копіювання даних.

Процес Маркова застосовується для опису моделі атаки на хмарне середовище та використовується CVSS для визначення запропонованої матриці переходу Маркова. Загрози безпеці є випадковим процесом і моделюється як ланцюг Маркова. Імовірність переходу з одного стану в інший базується на вразливостях, присутніх у поточному стані. Зловмисники використовують різні вразливості, щоб досягти стану загрози безпеці та, зрештою, остаточного стану відмови. На цьому етапі в основному зосереджуємось на абстракціях першого рівня з видимим і кількісно визначеним станом і конструкціями.

Виокремлюємо три стани: безпечний стан (S), стан загрози (T), стан несправності (F). На рисунку 1.2 представлено запропоновану модель Маркова для моделювання загроз безпеці та атак з використанням ймовірностей переходу стану, де α представляє ймовірність переходу зі стану S у стан T, β представляє ймовірність переходу від T до S, γ представляє ймовірність

переходу стану від T до F, δ представляє ймовірність переходу зі стану F назад у стан T, а ε представляє ймовірність переходу зі стану F назад у стан S.

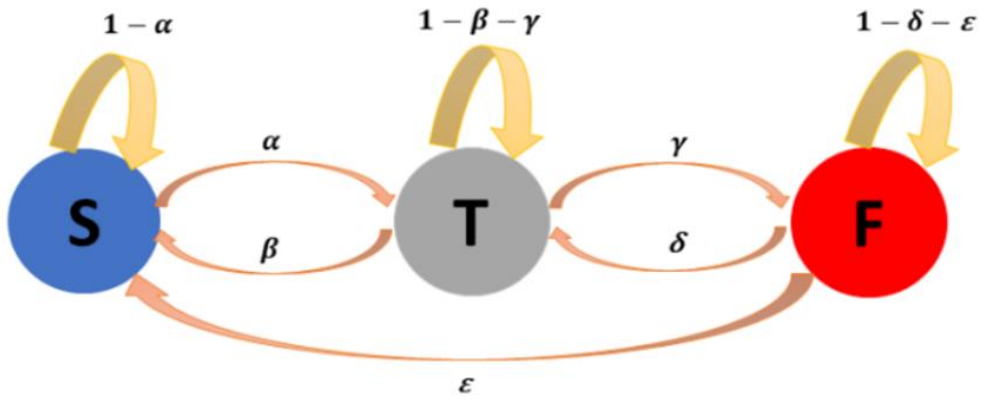


Рисунок 1.2 – Схема моделі атаки із захистом і відновленням [57]

Модель враховує всі елементи моделі атаки, включаючи фактори атаки, захисту та відновлення системи.

Не наводимо ймовірність прямого переходу зі стану S у стан F з ряду причин. По-перше, вивчаємо вплив загроз безпеці на системні збої та те, як зловмисники використовують загрози безпеці. Зловмисник намагається використати вразливість, щоб змінити стан безпеки на стан загрози. По-друге, система виходить з ладу (безпосередньо від S до F), зазвичай, у разі стихійних лих або подібних катастроф. У нашому випадку модель проста і практична. Навіть з цією моделлю з трьома станами важко вивести набір даних, щоб повністю описати його.

На рисунку 1. 3 представлена модель атаки з вбудованим захистом у стані відмови. Це означає, що немає ймовірностей переходу від F до T або від F до S. Коли процес досягає F, він залишається там з імовірністю 1. Це означає, що процес відновлення не розглядається.

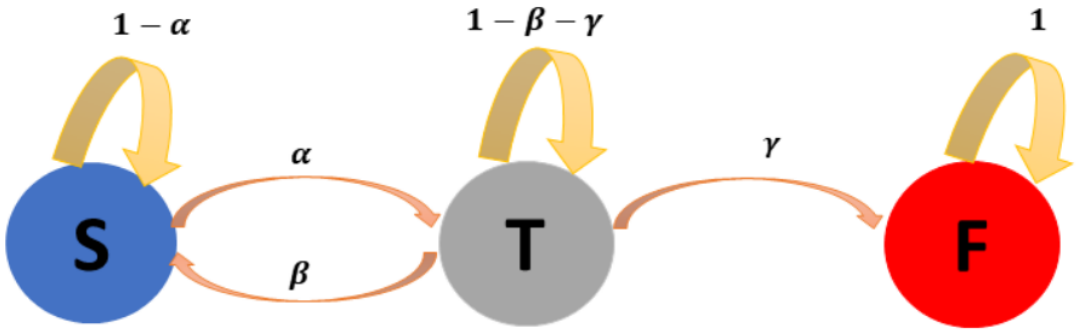


Рисунок 1.3 – Схема моделі атаки із захистом і без відновлення [57]

На рисунку 1. 4 представлена модель атаки зі вбудованими механізмами захисту в стані загрози та стані відмови. Саме на цій абстракції моделі зосереджуємося. Мета полягає в тому, щоб обчислити ймовірність використання зловмисником вразливості загрози для успішної атаки. Крім того, зусилля з відновлення, значною мірою, залежать від системних адміністраторів, і відповідні дані часто не розголошуються. Імовірність від S до T також означає загальну ймовірність спроби системи змінити стан із T назад до S, включаючи елементи захисту.

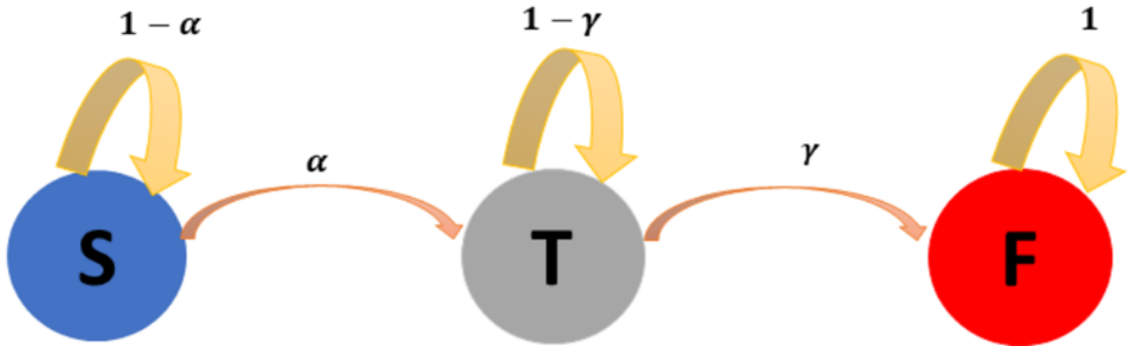


Рисунок 1.4 – Схема моделі атаки без захисту та відновлення [57]

Розглянемо визначення ймовірності переходу зі стану S у стан F у послідовності атаки. Рівняння Чепмена-Колмогорова [72] можна використовувати для розрахунку ймовірності переходу між двома станами після кількох кроків стрибка.

Як тільки розподіл ймовірностей станів ланцюга Маркова стає дискретним, а простір однорідним, його можна показати за допомогою множення матриці. Для того, щоб отримати ймовірність переходу між двома

станами за кілька кроків, можна використовувати рівняння Чепмена-Колмогорова за формулою (1.18).

$$P_{ij}^{m+n} = \sum P_{ik}^{m} P_{kj}^{n} \qquad (1.18)$$

де P – матриця ймовірностей переходу простору станів,

P_{ij}^{m+n} – ймовірність переходу зі стану і до стану j після $(m + n)$ кроків через будь-який стан *k*.

1.2.4 Основні стандарти у галузі ризиків

Все більше статистичних агенцій досліджують можливість складання офіційної статистики з використанням великої кількості джерел даних. Наразі є декілька прикладів повної інтеграції цих джерел у фактичну статистичну обробку даних. Тому наслідки такого злиття залишаються абсолютно невідомими. Водночас, це перша спроба проаналізувати умови та вплив великих даних на різні аспекти статистичної обробки даних, такі як якість чи методологія.

Відповідно до ISO 31000:20095 [75] ризик визначається як «вплив невизначеності на цілі». Це означає, що цілі повинні бути визначені або зрозумілі до того, як можна буде визначити ризики. Визначення цих цілей зазвичай бере до уваги інституційний контекст відповідної організації. Важливо також зазначити, що ризик характеризується невизначеністю того, чи відбудеться подія, чи ні. Таким чином, ризик вимірюється з точки зору ймовірності події та її наслідків, тобто впливу заходу на досягнення заданої мети [74].

Запропонована структура якості статистичних даних для джерел великих даних забезпечує структуроване уявлення про якість, пов’язану з усіма етапами статистичних бізнес-процесів, і, отже, може служити основним джерелом для комплексної оцінки та управління ризиками, пов’язаними з цими новими джерелами інформації. Вона вводить нові якісні показники, які є специфічними або дуже важливими при використанні великих даних для

офіційної статистики, наприклад, інституційне/ділове середовище. Використовуючи ці нові якісні показники, можна систематично визначати ризики, пов'язані з використанням джерел великих даних в офіційній статистиці.

Зосереджуючись на запропонованому вимірі якості, можемо описати ризики, які наразі не існують або впливають на офіційну статистику. Водночас, використовуючи великі дані для статистики, можемо ідентифікувати ризики, які сьогодні оцінюються по-різному.

Наступний етап – перехід до циклу управління ризиками, оцінюючи ймовірність і вплив цих ризиків. Оскільки оцінка ризиків передбачає суб'єктивне визначення ймовірності та впливу різних ризиків, незалежно оцінюються угоди між десятками різних зацікавлених сторін.

Потім пропонуються варіанти зменшення цих ризиків у чотирьох основних категоріях: уникнення, пом'якшення, розподіл та стримування [74].

Відповідно до ISO 31000:20095 одним із принципів управління ризиками має бути створення цінності [75]. Тобто для зменшення ризику слід використовувати менше ресурсів: не залучати ресурси, які використовувати недоцільно. Дотримуючись цього принципу, розберемо можливий вплив деяких заходів зі зменшення ризику на якість кінцевих результатів, щоб зробити більш комплексну оцінку використання великих даних в офіційній статистиці.

Як і багато інших секторів, офіційна статистика лише нещодавно почала обговорювати принципи застосування великих даних на стратегічному рівні [73]. Було проведено модернізацію моделей статистичної обробки даних і надання статистичних послуг на високому рівні, а також зроблено приблизний аналіз співвідношення ризик/вигода. «Комплексний аналіз ризиків також включатиме такі аспекти, як ймовірність й вплив, і може бути розширений для визначення стратегій пом'якшення ризиків і управління ними», – йдеться у звіті [73]. Хоча цей документ далекий від повного аналізу ризиків, він спрямований на покращення ситуації.

1.3 Уразливості, загрози та інциденти в кіберсистемах

1.3.1 Основні поняття

Уразливості найчастіше пов’язані з вадами захисту інформаційних та кібернетичних систем. Нижче наведені схеми класифікацій вад захисту та їх появи в системі [54] (рисунок 1.5 та 1.6).

Рисунок 1.5 – Класифікація вад захисту за етапами їх появи [54]

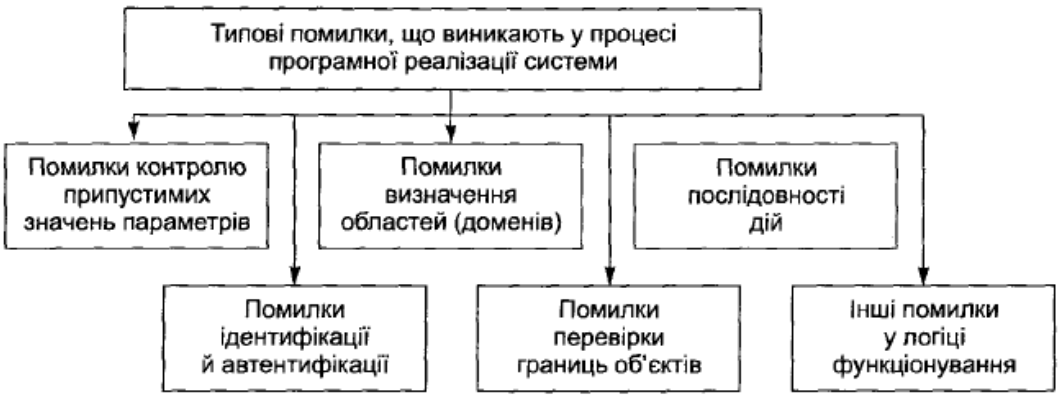


Рисунок 1.6 – Класифікація помилок, що виникають у процесі програмної реалізації системи [54]

Наведемо основну термінологію з питань інформаційної безпеки, яку будемо використовувати в подальшому дослідженні [54]:

Несприятливий вплив (англ. – undesired event) – вплив, що призводить до зменшення цінності інформаційних ресурсів.

Загроза (англ. – threat) – будь-яка обставина чи подія, що може спричинити порушення політики безпеки інформації та (або) нанесення збитку ІКС. Тобто загроза – це будь-який потенційно можливий несприятливий вплив.

Атака (англ. – attack) – це спроба реалізації загрози. Якщо атака є успішною (здійснено подолання засобів захисту), її називають проникненням (англ. – penetration). Наслідком успішної атаки є порушення безпеки інформації в системі, яке називають компрометацією (англ. – compromise).

Слід звернути увагу на те, що за умови комплексного підходу до захисту інформації мають розглядатися не лише впливи, спрямовані на інформаційні ресурси, але й будь-які впливи, що можуть завдати шкоди ІКС. Було вказано про необхідність захисту не самої інформації, а, насамперед, технології її оброблення.

Уразливість системи (англ. – system vulnerability) – нездатність системи протистояти реалізації певної загрози або ж сукупності загроз.

Вади захисту (англ. – security flaw) – сукупність причин, умов і обставин, наявність яких може призвести до порушення нормального функціонування системи або політики безпеки інформації. Здебільшого під вадами захисту розуміють особливості побудови програмних (а іноді й апаратних) засобів захисту, що за певних обставин спричиняють їхню нездатність протистояти загрозам і виконувати свої функції. Тобто вади захисту є окремим випадком уразливості системи.

У літературі іноді використовують інше тлумачення цих термінів, що, на наш погляд, не є коректним. Наприклад, часто замість терміну загроза вживають термін атака. Однак потрібно розрізняти атаку, яка є дією, тобто спробу реалізувати певну загрозу, та загрозу, яка робить потенційно можливим здійснення несприятливого впливу. Атака – це здебільшого цілеспрямований вплив, як правило, умисний. Загрози можуть бути

випадковими, хоча втрати від них не стають меншими. Тому захищати інформацію потрібно також від загроз, а не лише від атак.

Порушник (англ. – user violator) – фізична особа (не обов'язково користувач системи), яка порушує політику безпеки системи. Іноді використовують термін зловмисник (англ. – intruder), чим наголошують на умисності здійсненого ним порушення, тоді як порушник може здійснювати порушення ненавмисно (наприклад, через необережність або недостатню обізнаність).

Часто вживаний термін хакер (англ. – hacker) є доволі неоднозначним, тому не використовуватимемо його як синонім терміну порушник.

Модель [політики] безпеки (англ. – security policy model) – абстрактний формалізований чи неформалізований опис політики безпеки. Модель безпеки використовують під час проектування системи для визначення механізмів і алгоритмів захисту, а також під час аналізу захищеності системи для перевірки й доведення коректності та достатності реалізованих механізмів.

Модель загроз (англ. – model of threats) – абстрактний формалізований чи неформалізований опис методів і засобів здійснення загроз.

Модель порушника (англ. – user violator model) – абстрактний формалізований чи неформалізований опис порушника.

Моделі загроз і порушника є вихідною інформацією для розроблення політики безпеки і проектування будь-яких систем захисту.

Захищена комп'ютерна система (англ. – trusted computer system) – комп'ютерна система, що здатна забезпечувати захист оброблюваної інформації від визначених загроз. Цей термін частіше вживають до обчислювальних систем або їхніх складових (програмних продуктів, окремих програмно-апаратних пристроїв). Іноді його застосовують до ІКС, але потрібно розуміти, що будь-яка сучасна ІКС має бути захищеною (навіть домашній комп'ютер із одним користувачем). Інакше її використання дуже швидко призведе до втрат інформації.

Спостережуваність (англ. – accountability) – властивість ІКС, що дає змогу фіксувати діяльність користувачів і процесів, використання пасивних об’єктів, а також однозначно встановлювати ідентифікатори причетних до певних подій користувачів і процесів із метою запобігання порушенню політики безпеки і (або) забезпечення відповідальності за певні дії. Це дуже важлива властивість обчислювальних систем та ІКС, яка досягається реалізацією засобів реєстрації, або аудита (англ. — audit, auditing).

1.3.2 Графи та дерева атак

Дерева атак є методологією для опису загроз і способів протидії захисту системи. У розгорнутому вигляді схема дозволяє наочно уявити безпеку системи та дає можливість прорахувати захист, порівняти методи захисту різних систем тощо. Основна ідея полягає в тому, що за допомогою дерева атак можна виконувати опис варіантів здійснення атаки для досягнення певної мети, яка розташована на чолі дерева атак (є його вершиною). Кожен вузол дерева являє собою деяку підціль, досягнення якої при виконанні низки умов дозволяє зловмиснику піднятися по дереву на вищий рівень. І так доти, поки зловмисник не досягне вершини дерева (кінцевої мети). Приклад дерев атак наведено на рисунку 1.7.

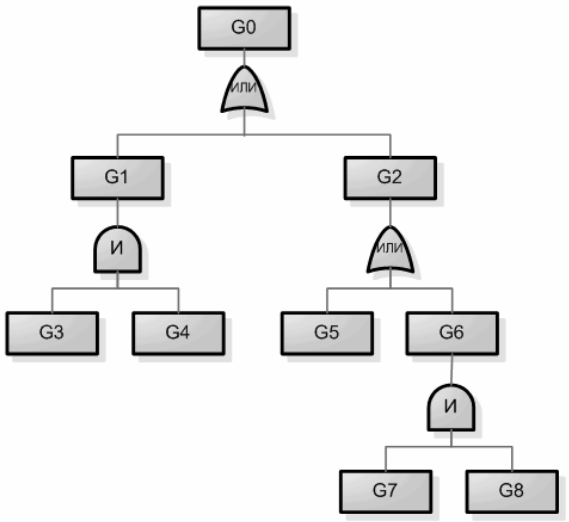


Рисунок 1.7 – Дерево атак

Якщо приписати кожному з вузлів дерева деякі значення, то це дозволить виконувати деякі розрахунки. Така схема називається «деревом І/АБО». Використовуючи дерева атак, можна не лише розробляти варіанти кібератак і визначати найбільш небезпечні сценарії, а також розробити контрзаходи проти них. Кожен із варіантів кібератаки має бути закритий контрзаходом (на рисунку 1.8 наведено контрзаходи С1, ..., С4). Деякі контрзаходи можуть закривати відразу кілька варіантів (наприклад, для підцілі G4 і G5 – контрзахід–С2), а для деяких варіантів потрібно використовувати кілька контрзаходів (для підцілі G5 - контрзаходи С2 і С3) [55]. Якщо модель системи захисту з повним перекриттям давала нам лише загрози та відповідні механізми захисту, які їх перекривають, у вигляді списку, то за допомогою дерева атак з'являється можливість будувати ієрархічну декомпозицію, досліджувати залежності, аналізувати різні сценарії атак та оптимально планувати розміщення механізмів захисту. Недоліком дерев атак є те, що з їхньою допомогою не можна описувати структури графів, які можуть містити цикли та повторювані елементи.

Поняття графа атак виникло унаслідок проекції більш загального поняття графа сценаріїв на область захисту інформації. Граф атак – це такий граф сценаріїв, у якому кожен шлях представляє атаку, тобто спосіб, яким зловмисник (порушник) може втрутитися у діяльність системи.

Існує багато робіт, присвячених побудові та аналізу СЗІ з використанням графів атак [91-94]. Головна перевага даного підходу полягає в тому, що за допомогою графа атак для чинної ІКС вдається дуже точно змоделювати можливі варіанти проникнення зловмисників у систему.

У роботі [90] автори розглядають два алгоритми для генерації графів сценаріїв. Перший з них базується на символічній перевірці моделі, а результат його роботи виражається в термінах логіки дерева обчислень. Інший алгоритм використовує аналіз чистих станів системи, та результат його роботи формулюється у термінах лінійної темпоральної логіки. Також можна визначити набір властивостей, які відповідають захищеному стану системи, і

для кожної з цих властивостей побудувати граф сценаріїв, що призводять за одним із алгоритмів до порушення даних властивостей.

Об’єднання цих графів сценаріїв і становитиме граф атак для системи. Будувати граф атак для системи можна вручну, але цей спосіб трудомісткий і отриманий граф може мати помилки, тому доцільно застосовувати автоматичні способи його побудови, особливо якщо йдеться про кібератаки.

Граф кібератак може слугувати відправною точкою для аналізу безпеки мережі в різних напрямках: виявлення вторгнень, захист, розслідування, додавання інцидентів тощо.

Графи кібератак можуть бути використані:

– для збору інформації про те, до яких атак система є уразливою і скількома способами зловмисник може досягти своєї мети;

– прийняття рішень щодо запобігання атак та вибору метрик безпеки.

За допомогою збудованого графа можна визначити пріоритетність покриття тієї чи іншої вразливості, візуально відобразити можливі шляхи атак або визначити задані метрики безпеки.

Автори детально розглядають два способи аналізу графів атак: видалення однієї вершини (дії) та мінімізацію критичного набору дій [90]. Перший спосіб дозволяє визначити ефект від видалення окремої дії з арсеналу зловмисника, другий – визначає набір дій, які слід заблокувати, щоб запобігти досягненню зловмисником своєї мети.

1.3.3 Топологічний аналіз уразливостей

У рамках традиційного підходу до аналізу захищеності ІКС кожна атака розглядається окремо. Це не відповідає справжньому стану, коли порушник намагається комбінувати різні атаки для досягнення своєї мети. Для реалістичного моделювання захищеної системи необхідно розглядати взаємозв’язки між різними атаками і вразливістю.

Топологічний аналіз уразливостей, запропонований Р. Тростом, базується на використанні графів атак і дозволяє зібрати інформацію про

захищеність мережі з урахуванням різних шляхів проникнення зловмисника у мережу [95].

Загальна структура підходу наведена на рисунку 1.8. Першим кроком є побудова моделі атаки на підставі даних про конфігурацію мережі та наявних уразливостей. Дані конфігурації мережі можуть включати звіти сканера вразливостей, результати інвентаризації мережі, правила, визначені на брандмауері тощо [104]. Після цього будується граф атак, який враховує як одною, так і багатокрокові атаки.

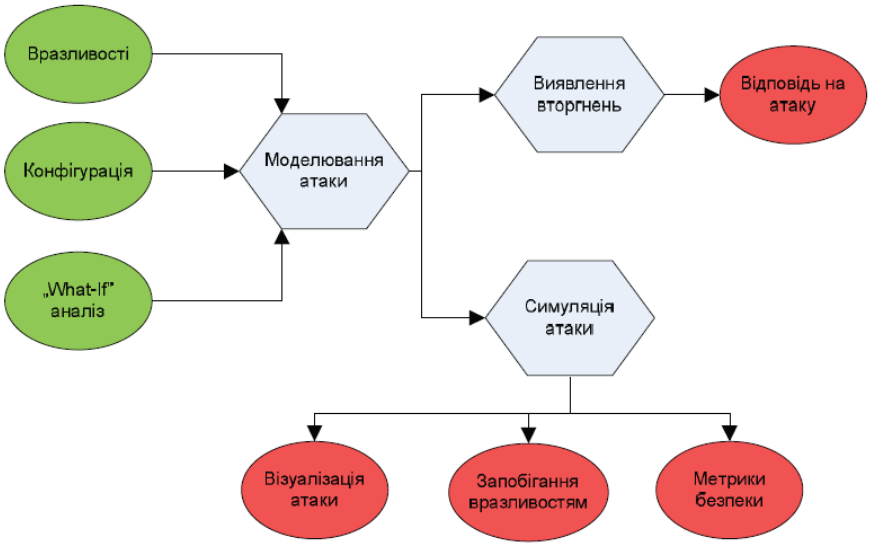


Рисунок 1.8 – Загальна схема застосування топологічного аналізу вразливостей

Топологічний аналіз уразливостей може бути застосований для багатьох типів систем та атак, включаючи і не пов'язані з ІКС. Якщо ж мати на увазі моделювання саме комп’ютерної мережі, то автори пропонують мережу як сукупність хостів, розділених на так звані домени захисту (protection domains). Хости, що знаходяться в одному домені захисту, мають необмежений доступ до сервісів (у тому числі й уразливих). Такий підхід є альтернативою наявності пов’язаних повністю підграфів у графі атак. Також домени можуть бути вкладені.

Кожен хост мережі включає ряд елементів та атрибутів, важливих для поділу мережевих атак. Прикладами таких атрибутів можуть бути операційна

система, зв’язки з уразливими сервісами на інших хостах, хости, яким даний хост довіряє тощо. Окремими атрибутами слугують засоби захисту. У рамках цього підходу вважається, що ефективність засобу захисту абсолютна, тобто при його наявності для певної вразливості, вона повністю виключається з графа атак.

Як уже зазначалося вище, дані про структуру мережі можуть збиратися автоматично, так само дані про вразливість можна отримувати зі спеціалізованих баз даних. Таким чином, людині, яка виконує побудову графа атак, залишається задати лише хости джерела загроз і критичні хости, на які спрямована атака. Після цього програмний засіб автоматично будує граф атак для мережі.

Після створення графа атак автоматично створюється список компонентів мережі, на яких слід встановити додаткові засоби захисту, для того, щоб підвищити захищеність цільових хостів. Одним із варіантів є посилення захисту безпосередньо джерела атаки. Інший спосіб – посилення захисту критичних ресурсів. У всіх випадках можна легко побачити, скільки вразливостей слід закрити для того, щоб досягти вищого рівня захищеності. Відтак, виходячи з цього, вибирається найефективніший спосіб захисту. Наприклад, для мережі, зображеної на рисунку 1.9, найбільш ефективним по кількості вразливостей, які потрібно закрити, буде третій варіант захисту.

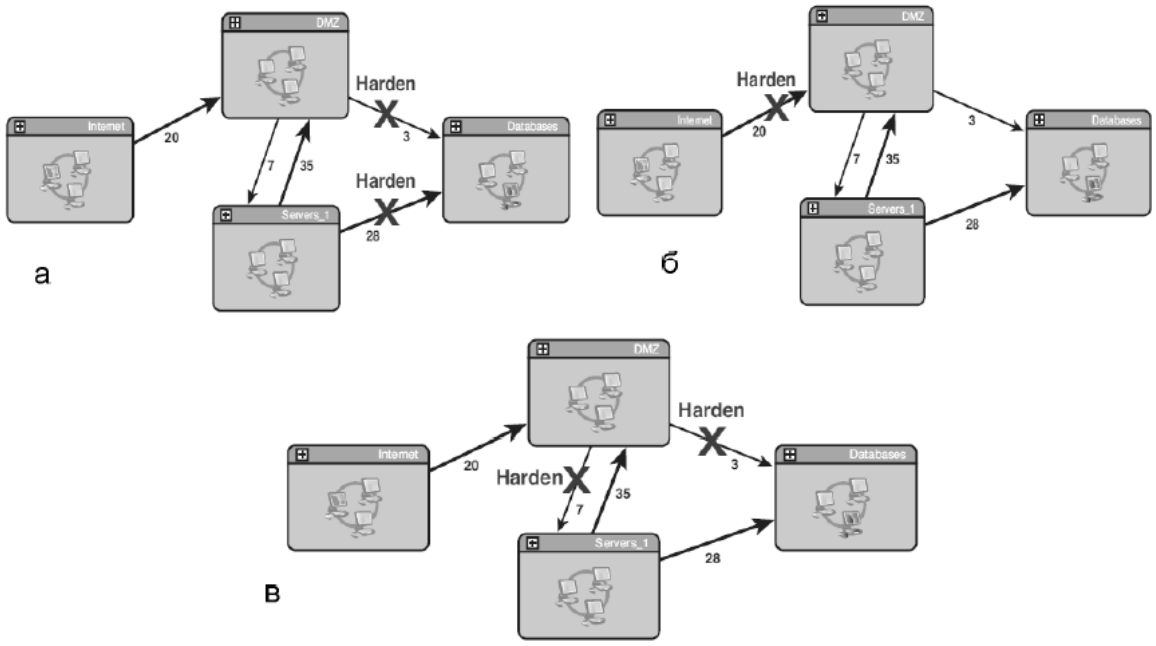


Рисунок 1.9 - Посилення захисту (а) мети атаки, (б) джерела атаки, (в) проміжних елементів – найбільш ефективний за кількістю уразливостей варіант

Цей підхід, наприклад, дозволяє визначити, де слід розмістити сенсори IDS, щоб покрити всі шляхи атак мінімальною кількістю сенсорів. Також, знаючи шляхи атак, можна відфільтровувати помилкові повідомлення про вторгнення [55]. Побудований граф атак дозволяє зіставляти окремі сигнали тривоги та розглядати їх як частину великої багатокрокової атаки. Тобто застосування топологічного аналізу вразливостей може зробити реакцію на атаки більш ефективною, одночасно мінімізуючи кількість помилкових тривог і вартість системи захисту.

Водночас, топологічний аналіз уразливостей містить засоби тільки для моделювання/симуляції атак і, як будь-який засіб моделювання, вимагає вхідних даних, тому ефективність такого моделювання безпосередньо залежить від ефективності існуючих інструментів для збору інформації про конфігурацію мережі та наявні уразливості [108]. Якщо вхідні дані будуть неповними, то й отриманий граф атак теж буде містити не всі можливі шляхи атак. Крім того, при моделюванні атак доводиться обмежувати детальність цієї моделі, щоб її обчислювальна складність залишалася в розумних межах [55].

1.3.4 Життєвий цикл уразливостей кіберсистем

Для визначення основних етапів життєвого циклу вразливостей наведемо основні проблеми пов'язані з цим процесом. Для аналізу проблем кібербезпеки, з якими стикаються компанії нині, необхідно отримати реальні дані і докази того, що конкретно відбувається у цій сфері [53]. Не у всіх галузях будуть однакові проблеми в області кібербезпеки. З цієї причини ми перерахуємо загрози, які зазвичай найбільш поширені в різних галузях. Це видається найбільш прийнятним підходом для аналітиків кібербезпеки, які не спеціалізуються на певних галузях, але в якийсь момент своєї кар'єри їм, можливо, доведеться мати справу з розділенням галузі.

Однією з найбільших проблем у цій сфері є ідентифікація зловмисників (порушників), коли вони вже знаходяться в мережі. Традиційних систем виявлення, таких як системи виявлення вторгнень (далі – IDS), може бути недостатньо, але вони можуть добре попередити про підозрілу активність, особливо якщо трафік зашифровано. Багато експертів відзначають, що між проникненням і виявленням може пройти до 229 днів [54]. Подолання цього розриву, безсумнівно, є одним із найважливіших завдань для фахівців із кібербезпеки.

Для підвищення рівня безпеки необхідно переконатися, що охоплені всі фази життєвого циклу атаки з точки зору захисту і виявлення. Але єдиний спосіб зробити це – переконатися, що є розуміння того, як працює кожен етап, як мислить зловмисник (порушник), і які можуть бути наслідки.

Наведемо етапи життєвого циклу вразливостей та загроз:

1. Інвентаризація ресурсів.

Першим етапом стратегії управління вразливими групами має бути інвентаризація. Однак багато організацій не мають ефективних реєстрів ресурсів, через що їм важко захистити свої пристрої. Інвентаризація активів – це інструмент, який адміністратори безпеки можуть використовувати для перевірки пристроїв, доступних в організації, і виокремлення тих, які мають бути захищені програмним забезпеченням. Що стосується стратегії управління

вразливістю, організації повинні почати з того, щоб визначити співробітника, відповідального за інвентаризацію ресурсів, аби гарантувати, що всі зареєстровані пристрої та результати інвентаризації актуальні. Інвентаризація ресурсів також є чудовим інструментом, який мережеві та системні адміністратори можуть використовувати для швидкого пошуку та налагодження пристроїв і систем. Без неї деяке важливе обладнання може бути забуте під час виправлення або встановлення нового програмного забезпечення для забезпечення безпеки. Ці пристрої та системи стають слабкою ланкою та мішенню для порушників.

Інвентаризація дозволяє більш ефективно оцінювати наявні запаси ресурсів, що, у свою чергу, дозволяє більш ефективно визначити необхідні обсяги коштів для забезпечення їх захисту. Адміністратор має можливість чітко ідентифікувати пристрої та системи, для яких необхідно придбати та встановити системи захисту.

На цьому етапі виникає низка питань. IT-відділи в сучасних організаціях часто стикаються з відсутністю оперативної інформації щодо зміни обладнання, серверів, які використовуються, та чітких меж мережі. Організаціям також не вистачає ефективних інструментів для постійного оперативного обліку ресурсів.

2. Управління інформацією.

Другий етап стратегії управління вразливістю полягає в контролі надходження інформації в організацію. Найважливішою інформацією є Інтернет-трафік з мережі організації. Зросла кількість «хробаків», «вірусів» та інших шкідливих програм, від яких потрібно захиститися. Також спостерігається збільшення трафіку як всередині, так і поза локальною мережею. Збільшення трафіку створює ризик швидкого поширення вірусних програм. Тому, слід звернути увагу на наявні інформаційні потоки, щоб запобігти проникненню загроз із мережі. Крім загрози застосування зловмисного програмного забезпечення, управління інформацією стосується даних організації. Організації зберігають різні типи даних, деякі з яких мають

конфіденційний характер. Якщо хакер отримує доступ до комерційної таємниці та особистої інформації клієнта, це може завдати непоправної шкоди. Організації можуть втратити свою репутацію і навіть отримати значні штрафи за неспроможність забезпечити належний захист даних клієнтів. Організації-конкуренти, які отримують доступ до секретних формул, прототипів і комерційних таємниць, мають можливість випередити компанії, які стали жертвами злому.

Організації можуть створювати групи реагування на інциденти з комп'ютерної безпеки для вирішення будь-яких ситуацій, якими інформація про загрози належними чином документується, зберігається та передається (2). Вищезазначені команди не лише реагують на випадки злому, але й інформують керівництво, коли хтось намагається отримати доступ до секретних даних. Фахівці також визначають найбільш відповідні заходи, які необхідно вжити у цих випадках. На додаток до цієї команди організації також можуть застосовувати політику обмеження доступу до окремої, визначеної інформації. Ця політика гарантує, що користувачам забороняється доступ до будь-якої інформації, окрім тієї, яка потрібна для виконання їхніх обов'язків. Обмеження кількості людей, які мають доступ до секретної інформації, є хорошим способом зменшити негативні наслідки у разі хакерського нападу.

Нарешті, стратегія управління інформацією організації може включати механізми виявлення та запобігання зловмисному доступу до файлів. Ці механізми можуть бути реалізовані в мережі, щоб запобігти проникненню зловмисного трафіку та забезпечити сповіщення про наявність підозрілої активності, такої як стеження (переслідування). Їх також можна встановити на пристрої кінцевих користувачів, щоб запобігти незаконному копіюванню або зчитуванню даних.

Існує декілька проблем із поточними стратегіями управління вразливістю. Почнемо з того, що останнім часом обсяги інформації швидко зростають, що ускладнює їх обробку, використання та контроль доступу до них. Цінна інформація, наприклад, повідомлення, пов'язана з можливими

порушеннями, яку також не в змозі обробити більшість IT-відділів. З огляду на велику кількість подібних повідомлень, які IT-спеціалісти отримують щодня, не дивно, що повідомлення, пов'язані з можливими кібератаками, інколи вважаються помилковими. У деяких випадках організації піддавалися атаці незабаром після того, як вони ігнорували попередження від інструментів моніторингу мережі.

Не можна звинувачувати IT-відділ у цьому, адже такі інструменти щогодини генерують тони нової інформації, більшість з якої є помилковою. Трафік мережі організації також може бути ускладненим. Шкідливі програми починають поширюватися нетрадиційними способами. Також виникає проблема при передачі інформації про нові вразливості звичайним користувачам, які не розуміють технічної термінології. Усі ці проблеми впливають на час реагування на дії, які організація вживатиме у випадку потенційного чи доведеного порушення.

3. Оцінка ризику.

Перш ніж усунути ризик, команда безпеки повинна виконати поглиблений аналіз уразливостей, з якими вона стикається. В ідеальному IT-середовищі служби безпеки можуть реагувати на всі порушення, оскільки мають достатньо ресурсів і часу. Однак на практиці існує багато обмежень щодо ресурсів, доступних для подолання ризиків. Ось чому оцінка ризику має вирішальне значення. На цьому етапі організації повинні визначити пріоритети певних уразливостей і виділити ресурси для їх усунення. Одним із принципів управління ризиком описаний в [101].

4. Сфера застосування.

Оцінка ризику починається з визначення його обсягу (зони дослідження), відповідальної команди, наявного бюджету. Тому керівники повинні визначити, які сфери охоплюватимуться, а які ні. Вони визначають, які ресурси мають бути захищені, їх чутливість і необхідний рівень захисту. Обсяг (зону дослідження) слід ретельно вивчити, оскільки він має визначити, де необхідно проводити аналіз внутрішніх і зовнішніх уразливостей.

5. Збір даних.

Після визначення масштабу необхідно зібрати дані про існуючі політики та процедури, які захищають організацію від кіберзагроз. Це можна зробити за допомогою інтерв'ю, анкет та опитувань користувачів та адміністраторів мережі. Про усі мережі, додатки та системи, що знаходяться в зоні дослідження, повинні бути збирані відповідні дані. Ці дані можуть включати пакети оновлень, версії операційної системи, запущені програми, місцезнаходження, дозволи контролю доступу, тести виявлення вторгнень, тести брандмауера, дослідження мережі та сканування портів. Ця інформація дозволить краще зрозуміти типи загроз для мережі, систем і програм.

Також ефективним заходом може бути розвідка на основі моніторингу відпрацьованих ресурсів. Необхідно не забувати правильно утилізувати застаріле обладнання, не допустити втрати або несанкціонованого збору даних сторонніми особами.

6. Аналіз політики та процедур.

Організація розробляє політику та процедури для управління своїми ресурсами. Вона забезпечує правильне та безпечне їх використання. Тому важливо переглянути та проаналізувати існуючі політики та процедури. Деякі політики також можуть бути непрактичними. Аналізуючи політику та процедури, необхідно визначити, наскільки користувачі та адміністратори дотримуються вимог, визначених відповідними документами. Розробка та розповсюдження політики та процедур не означає, що їх будуть дотримуватись. Слід також передбачити покарання за невиконання. Згодом стане зрозуміло, чи має організація достатню політику та процедури для усунення вразливостей.

7. Аналіз вразливостей.

Наступним кроком після аналізу політик і процедур є аналіз уразливості задля знаходження вразливих місць інформаційної системи організації та визначення адекватних засобів її захисту.

Тестери проникнення повинні моделювати атаки в реальному часі та вчасно ідентифікувати скомпрометовані системи та пристрої. Нарешті, виявлені вразливості класифікуються відповідно до ризику, який вони становлять для організації. Уразливості, які виявляють менш чутливі слабкі місця, зазвичай, мають нижчі рейтинги.

Системи оцінки вразливості діляться на три категорії. Нижча категорія визначена для вразливостей, які потребують значних ресурсів для усунення, але мають незначний вплив на організацію. Середній рейтинг визначено для вразливостей із прийнятним потенціалом для усунення та впливу. Категорія високого рівня серйозності призначена для вразливостей, які потребують небагато ресурсів для усунення, але можуть нанести великої шкоди організації при їх наявності.

8. Аналіз загроз.

Загрозою для організації є операція, код або програмне забезпечення, які можуть призвести до підробки, знищення даних або припинення обслуговування. Аналіз загроз виконується для оцінки ризиків, які можуть виникнути в організації. Виявлені загрози необхідно проаналізувати, щоб визначити їхній вплив на організацію.

Загрози класифікуються подібно до вразливостей, але розглядаються з точки зору мотивації та можливостей. Наприклад, інсайдер може мати мало стимулів здійснювати атаки на організацію, але має багато можливостей, оскільки він знає, як організація працює всередині. Таким чином, рейтингова система може дещо відрізнятися від системи, що використовується в аналізі вразливостей. Відтак необхідно визначити кількість виявлених загроз та класифікувати їх.

9. Аналіз прийнятних ризиків.

Завершальним етапом є аналіз прийнятного ризику. Передусім аналізується існуюча політика безпеки, процедури та механізми, щоб визначити, чи вони адекватні. Якщо ні, припускається, що в організації існує вразливість. Здійснюється відповідне корегування до тих пір, допоки не буде

вирішено, що цього достатньо для забезпечення прийнятного рівня безпеки. ІТ-відділ визначає рекомендовані стандарти, яким має відповідати програма безпеки. Все, що до них не включено, класифікується як прийнятний ризик. Однак, з часом ці ризики можуть стати більш небезпечними, тому їх необхідно постійно аналізувати, та корегувати стандарти. Оцінка ризику проводиться до тих пір, поки не буде встановлено, що вразливості не становлять загрози. Якщо вони можуть становити загрозу, необхідно оновити стандарти безпеки, щоб їх усунути.

Найбільшою проблемою управління вразливістю на цьому етапі є обмеження доступної інформації. Деякі організації не документують свою політику, процедури, процеси та заходи безпеки, тому отримати інформацію, необхідну для виконання цього кроку, може бути важко. Для малих і середніх компаній значно легше документувати все, але для великих компаній – надзвичайно складно. У великих компаніях існує багато напрямків діяльності, відділів, брак ресурсів і впорядкованої документації, а також дублювання обов'язків. Єдиний спосіб підготувати їх до цього процесу – проводити регулярні офісні заходи (наради), щоб гарантувати, що все важливе задокументовано, а працівники чітко розуміють свої обов'язки.

10. Оцінка вразливості.

Оцінка вразливості тісно пов'язана з оцінкою ризику в стратегії управління вразливістю. Оцінка включає виявлення вразливих ресурсів. Цей етап виконується за допомогою серії скоординованих спроб несанкціонованого вторгнення та тестів на проникнення. Ці атаки спрямовані на сервери, принтери, робочі станції, брандмауери, маршрутизатори та комутатори в мережі організації. Мета полягає в тому, щоб імітувати сценарії несанкціонованого вторгнення в реальному часі за допомогою тих самих інструментів і методів, які може використовувати потенційний зловмисник.

Мета цього етапу полягає не лише у виявленні вразливостей, а й у тому, щоб зробити це швидко й точно. На цьому етапі є багато проблем. Перше, що необхідно зробити – це провести належну інвентаризацію ресурсів задля

виявлення пристроїв, що потребують захисту. Потрібно пам’ятати про безпеку окремих хостів, оскільки вони все також можуть бути ключовими цілями для потенційних атак. Ще одна проблема пов’язана з використанням сканеру вразливостей. Деякі сканери надають неправильні звіти про оцінку ризику та спрямовують організації хибним шляхом. Звичайно, завжди будуть помилкові спрацьовування, але деякі інструменти сканування виходять за межі прийнятного відсотка та все одно виявляють уразливості, яких не існує. Це може призвести до марної витрати організаційних ресурсів, коли справа доходить до заходів із зменшення вразливості.

Збої у роботі організації – ще один набір проблем, з якими дослідники стикаються на цьому етапі. Мережі, сервери та робочі станції стають уразливими через усі дії перевірки проти злому та тестування на проникнення. Мережеве обладнання, таке як брандмауери, також працює повільно, особливо коли виконуються атаки типу «відмова в обслуговуванні» [99].

Іноді потужна тестова атака може фактично вивести з ладу сервер, порушивши основні функції організації. Для уникнення таких ситуацій, необхідно проводити такі тести, коли користувачі не використовують сервер, або запропонувати альтернативи під час оцінювання основних інструментів безпеки. Іноді інструментам сканування не вистачає належних можливостей звітування, що змушує тестувальників проникнення писати ці звіти вручну.

11. Звітування та відстеження виправлень.

Наступною фазою після оцінки вразливості є фаза звітування про поточний стан інформаційної системи організації та виправлення інформаційної системи. Ця фаза має два однаково важливі завдання: звітування про стан та виправлення помилок. Ці звіти допомагають системним адміністраторам зрозуміти поточний стан безпеки в організації та сферах, які все ще залишаються вразливими, і вказати на це відповідальним особам. Звіти також забезпечують керівництво конкретним баченням, що стосується майбутнього управління організацією. Звіти зазвичай формуються до моменту

виправлення, щоб вся інформація, зібрана на етапі управління вразливостями, могла безперешкодно перетікати в фазу виправлення.

Виправлення вразливостей розпочинає фактичний процес завершення циклу управління вразливістю. Як зазначалося раніше, фаза управління вразливістю завершується аналізом загроз і вразливостей, а також визначенням прийнятного ризику. Патч доповнює це, надаючи рішення для виявлених загроз і вразливостей. Відстежуються всі вразливі вузли, сервери та мережеві пристрої, а потім вживаються необхідні дії для усунення вразливостей і захисту для подальшої експлуатації. Це найважливіше завдання в стратегії управління вразливістю, і якщо воно виконано досконало, управління вразливістю вважається успішним. Дії, які виконуються в цьому завданні, включають виявлення відсутніх виправлень і перевірку всіх систем в організації на наявність оновлень. Також приймається рішення щодо помилок, виявлених засобом сканування. На цьому етапі все ще наголошується на кількох рівнях безпеки, таких як антивірусні програми та брандмауери. Якщо ця фаза не виявилась ефективною, то весь процес управління уразливостями втрачає зміст.

Як і очікувалося, на цьому етапі виникає багато питань, оскільки саме тут визначаються шляхи вирішення всіх уразливостей. Перша проблема виникає у разі, коли звіт не охоплює всіх необхідних областей і не містить усієї необхідної інформації про ризики, з якими стикається організація. Погано написані звіти про поточний стан інформаційної системи можуть призвести до неналежного усунення вразливостей, та залишити організацію вразливою для загроз.

Відсутність необхідної програмної документації також може спричинити проблеми на цьому етапі. Постачальник або виробник програмного забезпечення зазвичай додає супроводжуючий документ із інструкціями щодо виконання його оновлення. У разі відсутності відповідних інструкцій програмне забезпечення буде важко оновити. Погана взаємодія між постачальниками програмного забезпечення та організаціями також може

спричинити проблеми, коли виникає необхідність повного оновлення системи. Нарешті, процес відновлення системи може постраждати через відсутність належної співпраці з кінцевими користувачами.

12. Планування реагування.

Планування реагування можна вважати найпростішим, але дуже важливим кроком у стратегії управління вразливістю. Це важливо, оскільки без цього організації продовжуватимуть стикатися з тими ж загрозами, що й раніше. На цьому етапі має значення тільки швидкість виконання. При наявності значної кількості пристроїв, які потребують виправлень і оновлень, великі організації стикаються з серйозними перешкодами.

Був інцидент, коли Microsoft оголосила про існування MS03-023 і випустила патч для нього. Невеликі організації з малими системами та планами швидкого реагування швидко оновили свої операційні системи. Однак великі організації, в яких були відсутні комп'ютерні плани реагування, або процес оновлення програмного забезпечення вимагав забагато часу, залишилися вразливими до несанкціонованого вторгнення.

Всього через 26 днів після того, як Microsoft випустила патч для своїх користувачів, хакери випустили вірусну програму MS Blaster для атаки на неоновлені операційні системи. Навіть для великих компаній було достаньмо часу, щоб повністю оновити своє програмне забезпечення. Однак, відсутність плану реагування або використання повільного плану реагування призвело до того, що деякі організації постраждали від несанкціонованого вторгнення. Вірусна програма викликала уповільнення або перебої в роботі заражених комп'ютерів.

Наведений вище приклад свідчить про те, наскільки важлива швидкість при плануванні реагування. Патчі слід встановлювати швидко, як тільки вони стають доступними.

Цей етап є складним, оскільки передбачає фізичну участь кінцевих користувачів та їхніх комп'ютерів. Перше завдання – вчасно донести важливу інформацію до зацікавлених людей. Після випуску виправлень хакери швидко

знаходять способи скомпрометувати організації, у яких програмне забезпечення залишилося не оновленим. Ось чому важливим є добре налагоджений зв’язок між організаціями та компаніями – постачальниками програмного забезпечення.

Інше питання – відповідальність. В організаціях повинні бути чітко визначені особи, які безпосередньо несуть відповідальність за швидке встановлення оновленого програмного забезпечення. В окремих організаціях користувач безпосередньо може нести відповідальність за оновленого програмного забезпечення. В інших випадках може статися, що відповідальною є IT-команда, яка не розпочала процес оновлення вчасно. Хтось завжди повинен нести відповідальність за вчасне встановлення патча.

Остання проблема – дублювання роботи. Це часто трапляється у великих організаціях, де великий штат співробітників IT-служби безпеки. Вони можуть використовувати єдиний план реагування, але через неналежну взаємодію – дублюють зусилля один одного, що значно знижує ефективне досягнення кінцевого результату.

Після підготовки плану відпрацювання вразливостей та загроз необхідно пам’ятати, що процес є динамічним. Нові вразливості можуть виникати і надалі, як і нові загрози. Нижче на рисунку 1.10, наведено орієнтовну схему життєвого циклу небезпеки в будь-якій кіберсистеми.

Рисунок 1.10 - Схема життєвого циклу небезпеки в кіберсистемі

У наступному пункті дослідження більш детально описано ймовірнісні моделі залежностей загроз та вразливостей.

1.4 Сучасні підходи до аналізу складних кіберсистем

1.4.1 Системи складної структури

Q-аналіз найчастіше використовується для дослідження складних систем [38]. Дефініція поняття «складної системи» в різних розділах науки відносно мало досліджена аналітично, проте вона широко обговорюється соціологами та філософами соціальних наук [41]. Наступні цитати (окрім останньої) взяті зі спеціального випуску журналу Science про «складні системи», де представлені визначення поняття «складність», які провідними науковцями [39].

1. «…Складність означає, що ми маємо структуру з варіаціями» [46].

2. «За однією характеристикою, складна система — це така, еволюція якої дуже чутлива до початкових умов або малих збурень, така, у якій кількість незалежних взаємодіючих компонентів є великою, або така, у якій існує кілька шляхів, якими система може розвиватися. Для аналітичного опису таких систем зазвичай потрібні нелінійні диференціальні рівняння. Друга характеристика є більш неформальною: тобто система «ускладнена» деяким суб'єктивним судженням і не піддається точному опису, аналітичному чи іншому» [39].

3. «У загальному розумінні прикметник «комплексний» описує систему або компонент, які важко зрозуміти та перевірити через функцію проектування або ними обома. [...] складність визначається такими факторами, як кількість компонентів і складність інтерфейсів між ними, кількість і складність умовних гілок, ступінь вкладеності та типи структур даних.» [42].

4. «Теорія складності вказує на те, що великі популяції одиниць можуть само організовуватися в агрегації, які створюють шаблон, зберігають інформацію та беруть участь у колективному прийнятті рішень» [40].

5. «Складність природних моделей рельєфу є проявом двох ключових характеристик. Природні моделі формуються з процесів, які є нелінійними, такими, що змінюють властивості середовища, в якому вони діють, або тісно пов'язані між собою; і природні закономірності утворюють відкриті системи, виведені з рівноваги завдяки обміну енергією, імпульсом, матеріалом або інформацією через їхні кордони» [43].

6. «Складна система — це буквально система, у якій є кілька взаємодій між багатьма різними компонентами» [40].

7. «Спільним для всіх досліджень складності є системи з декількома елементами, які адаптуються або реагують на шаблон, створений цими елементами» [47].

8. «Останніми роками наукове співтовариство визначило рубрику «складна система» для опису явищ, структури, агрегатів, організмів або

проблем, які мають спільну тему: (i) вони за своєю суттю є складними або заплутаними [...]; (ii) вони рідко є повністю детермінованими; (iii) математичні моделі системи, як правило, складні та включають нелінійну, неправильно сформульовану або хаотичну поведінку; (iv) системи схильні до неочікуваних результатів (так званої емерджентної поведінки)» [45].

9. «Складність починається, коли руйнується причинність» [44].

Остання цитата добре ілюструє труднощі цієї сфери. Зрозуміло, що багато людей матимуть досить стримане уявлення про причинність, щоб виявити наявність причинно-наслідкових зв’язків у складних системах. І, справді, багато людей стверджуватимуть, що головне завдання науки про складність – зрозуміти її.

Перше визначення може бути вірним, але навряд чи є інформативним, якщо не визначено, що мається на увазі під структурою та варіаціями.

Друге визначення пропонує вибрати між поєднанням науки про складність та хаосом і нелінійною динамікою, або поєднанням складності з великою кількістю компонентів, або поєднанням складності із системою з різними можливими історіями, з одного боку, і повністю суб’єктивною відповіддю на поставлене запитання.

Третє та четверте визначення пропонують більш цікаві об’єкти для вивчення. Обчислювальні поняття структур даних, умовних розгалужень і обробки інформації є центральними для науки про складність, і вони будуть мати центральне значення в розділах 3, 4 і 5.

П’яте визначення вводить центральну ідею не лінійності. Не зважаючи на те, що багато складних систем піддаються нелінійній динаміці, ця ознака не є ні необхідною, ні достатньою умовою складності.

Підтримується точка зору, наведена у шостому та сьомому визначеннях, згідно з якою система не може бути складною, якщо в ній не взаємодіє багато компонентів, але стверджується, що ця умова недостатня, і становить обмежений інтерес.

Восьме визначення вводить ідею появи, яка є занадто заплутаною, щоб бути частиною інформативної характеристики складної системи.

Здатність розуміти системи безпосередньо залежить від складності цих систем. Складність є потенційною «загрозою» для розуміння. Однак, коли з'являється розуміння самої складності, можемо оперувати цим поняттям при здійсненні аналізу.

Чітке визначення поняття «складності» дозволяє зрозуміти принципи функціонування складних систем. Це дозволяє переглянути поняття чорних ящиків і концепцію абстракції, щоб проілюструвати, що існують альтернативні способи управління складністю, які не вимагають значної деталізації [48].

Нижче наведено основні властивості складної системи.

• Складні системи часто демонструють мінливу поведінку. Неможливо легко передбачити, як складна система буде функціонувати, навіть за зовнішніх начебто однакових умов.

• Складні системи вимагають виконання значного обсягу роботи, щоб «зрозуміти» їх.

• Складні системи не можна легко описати, і, звичайно, не шляхом простого перерахування їх частин [49].

Усі складні системи демонструють деякі спільні характеристики:

1. Вони складаються з великої кількості взаємодіючих частин.

2. Вони виявляють емерджентність: самоорганізована загальна поведінка не завжди є складовою поведінки окремих частин.

3. Емерджентна поведінка складних систем не є результатом існування центрального контролера [50].

Властивості складних систем

Взаємна автономність елементів системи: кожному її елементу притаманні властивості системи в цілому.

Іманентність: системоутворююче взаємовідношення властиве лише для елементів цієї системи.

Множинність: одна і та ж сукупність елементів може бути множиною різних систем, які відрізняються системо-утворюючими властивостями та конкретними відношеннями між елементами. Наприклад, студентська група може розглядатися як навчальна система в освітньому процесі університету і як соціальна система взаємостосунків у колективі.

Надійність системи: здатність зберігати системоутворюючу властивість при елімінації (вилученні) деякої кількості елементів.

Завершеність системи: система не допускає приєднання нових зовнішніх елементів без руйнування цієї системи.

Мінімальність: руйнування при вилученні хоча б одного елемента.

Цілісність: система поводить себе як єдине ціле. Це означає, що, з одного боку, система – це цілісне утворення, а з іншого – в її складі чітко можуть бути виділені окремі об'єкти (елементи). Але не компоненти утворюють ціле (систему), навпаки, при поділі цілого виявляються компоненти системи. Первинність цілого – головний постулат теорії систем.

Емерджентність: складна система має такі властивості, які не притаманні жодному з її елементів.

Синергізм: ефективність спільного функціонування елементів системи є вищою, ніж сумарна ефективність ізольованого функціонування цих же елементів.

Еквіпотенційність: кожну систему можна розглядати як підсистему іншої більш крупної системи; кожен елемент системи, в свою чергу, є системою.

До властивостей, що формують здатність системи до самозбереження, належать:

– здатність зберігати рівноважний стан незалежно від умов зовнішнього середовища;

– здатність самостійно утримувати основні параметри в допустимих межах (цю властивість називають гомеостазом);

– здатність динамічно реагувати на зміни й впливи навколишнього середовища за рахунок структурних перебудов.

Відкриті складні системи мають низку характерних особливостей:

– диференціація – різні складові системи виконують різні функції і не є взаємозамінними (приклад: сторож, бухгалтер, програміст у системі організації);

– централізація – з часом одна зі складових системи може стати домінуючою (приклад: урядова бюрократія вимагає концентрації та централізації влади; для корпоративного підходу до управління більш характерним є децентралізація владних повноважень);

– цілеспрямованість – процеси можуть протікати по-різному, але кінцевий стан системи буде однаковим, тобто поведінка системи та її структура спрямовані на досягнення певної мети (приклад: струмки, що стікають зі схилу гори в озеро, яке розташоване в низині);

– історичність – система не може бути незмінною, вона виникає, функціонує, розвивається і зникає [51].

Останні книги з аналізу ризиків і надійності стосуються «складних систем», але (майже) жодна з них не визначає, що вони мають на увазі під терміном «складні».

Пропонується класифікувати систему в одну з трьох категорій.

– Просту систему легко зрозуміти і її можна проаналізувати, дотримуючись визначеної процедури або алгоритму. Більшість простих систем мають досить невелику кількість компонентів. Прості системи відповідають ньютонівсько-декартовій парадигмі.

– Складна система має велику кількість компонентів зі значним ступенем взаємозв’язків і взаємозалежностей між компонентами. Використовуючи сучасні знання (наприклад, залучаючи експертів з різних предметних сфер), можна зрозуміти відповідні властивості системи та проаналізувати їх. Відносини між компонентами можна звести до чітких, передбачуваних взаємодій. Складні системи можна декомпонувати у

відповідності до ньютонівсько-декартової парадигми. Прикладами складних систем є літаки та комп'ютери.

– У складній системі поведінка принаймні деяких компонентів або взаємодії між ними не є повністю зрозумілими, навіть якщо використовувати всі поточні знання. Продуктивність складної системи неможливо передбачити адекватно за допомогою лінійних залежностей. Складну систему неможливо адекватно зрозуміти й проаналізувати за допомогою традиційних підходів, оскільки система є чимось більшим, ніж сума її компонентів. А складна система не може бути декомпозована без втрати деяких характеристик, що не відповідає вимогам ньютонівсько-декартової парадигми. Деякі автори просто визначають складну систему як систему, яка не відповідає ньютонівсько-картезіанській парадигмі.

Отже, термін «складність» можна визначити так:

Поняття «складність» – це наукова теорія, яка стверджує, що деякі системи демонструють поведінкові явища, які абсолютно неможливо пояснити будь-яким звичайним аналізом складових частин системи [52].

Надалі використання термінів складність та складна система буде базуватися на наведеному вище визначенні. Основними методами опису складних систем є топологія та мережеві структури [106] (окремими випадком яким є гіперграфи).

1.4.2 Q-аналіз та його застосування в аналізі структури складних систем

Дослідження зв'язності і складності системи необхідно для прийняття рішень, вирішення завдань про можливість управління системою, вибору способів управління, оцінки ризиків і вразливостей.

Слабозв'язана система допускає селективне управління підсистемами, але, при цьому, дає можливість розмежовувати сфери діяльності підсистем та збільшувати захищеність від кібератак. Це може мати і негативні сторони через недотримання принципу системності.

Різні концепції зв'язності відображають єдину тенденцію – виявлення істотних, функціонально-значущих зв'язків системи, порушення або виникнення яких повністю змінює можливості досягнення цілей, можливості функціонувати, підвищувати вразливість.

У дослідженні для аналізу зв'язності системи із зовнішнім середовищем пропонується використовувати аналіз q-зв'язності системи [13].

Структура є зв'язною, якщо можливий обмін ресурсами між будь-якими двома підсистемами системи (передбачається, що якщо є обмін і-й підсистеми з j-й підсистемою, тобто і обмін j-й підсистеми з і-й також існує).

Методика аналізу q-зв'язності дозволяє робити висновки про структуру системи більш глибоко, ніж традиційні дослідження теорії графа, оскільки при цьому встановлюється наявність взаємовпливу підсистем через ланцюжок зв'язків між ними. На підставі таких можливостей пропонуються формалізовані правила обґрунтування вибору цільових і керуючих вершин, визначення стійкості систем, які характеризуються тими чи іншими симплеціальними комплексами, умовами структурної стійкості систем, визначенням числа симплексів і їх структури. Окрім того, аналіз q-зв'язності системи дозволяє висунути обґрунтування для вирішення завдань декомпозиції і композиції досліджуваної системи, виявити симплекси, які найбільше впливають на процеси в системі й окремі вершини, які раціональніше вибирати в якості керуючих [14].

Симплеціальні комплекси утворюють зв'язний, багатовимірний простір або структуру, і саме це є предметом дослідження *Q*-аналізу.

Розглянемо дві множини X та Y. Задаємо відношення λ між цими двома множинами елементів як підмножину декартового добутку $X \times Y$, де $\lambda \subset Y \times X$. Припустимо, що $Y = \{Y_1, Y_2, ..., Y_n\}$ та $X = \{X_1, X_2, ..., X_m\}$. Множина $Y = \{Y_1, Y_2, ..., Y_n\}$ пов'язана відношенням λ із множиною $X = \{X_1, X_2, ..., X_m\}$. Пара $(Y_i, X_j) \in \lambda$ та елемент множини Y_i знаходяться у відношенні λ до X_k, де $\lambda_{ij} = 1$ у разі виконання певного критерію і $\lambda_{ij} = 0$ у разі не виконання. Співвідношення між множинами елементів системи подається за допомогою матриці інцидентності

$\Delta = (\lambda_{ik})$, де $\lambda_{ik} = 1$, якщо $(Y_i, X_k) \in \lambda$ та $\lambda_{ik} = 0$, якщо $(Y_i, X_k) \notin \lambda$. Відношення λ породжує симплеціальний комплекс, що позначається через $K_Y(X; \lambda)$.

Симплеціальний комплекс складається із множини вершин X та множини симплексів Y, що утворені з цих вершин у відповідності із заданим бінарним відношенням λ. Зазначимо, що n-симплекс складається з n+1 вершин і його розмірність на одиницю менша від числа вершин.

Симплеціальний комплекс $K_Y(X; \lambda)$, утворений множиною симплексів Y, зв'язаних спільними гранями, тобто через спільні вершини.

Формально комплекс $K_Y(X; \lambda)$ визначається у такий спосіб:

– $K_Y(X; \lambda)$ є множиною симплексів $\{\sigma_p; p = 0,1,..., N\}$;

– кожний симплекс $\sigma_p \in K$ однозначно визначається деякою підмножиною з $(p+1)$ різних X_k, для нього існує принаймні одне $Y_n \in Y$, таке, що $(Y_n, X_k) \in \lambda$ для кожного з $(p+1)$ значень i;

– симплекс σ_{i0} ототожнюється з X_k, $i = 1,..., n$ (n — кількість елементів множини X);

– кожна підмножина симплекса σ_p, що визначається його $q+1$ вершинами ($q < p$), називається q-гранню симплекса σ_p й утворює $\sigma_p \in K$ (записується $\sigma_q < \sigma_p$).

Число N із пункту 1 називається розмірністю комплексу K та записується як dim K. Воно означає найбільшу розмірність для будь-яких $\sigma_p \in K$. Множина X також називається множиною вершин комплексу $K_Y(X; \lambda)$.

Загалом, p-симплекс σ_p представляється випуклим багатогранником із вершинами в евклідовому просторі E^p, а комплекс $K_Y(X; \lambda)$ — сукупністю таких багатогранників у евклідовому просторі E^α відповідної розмірності.

Складність системи також породжує проблеми аналізу довгих причинно-наслідкових зв'язків і циклів, а також складнощі в системі управління. Складність моделі також відображає тип невизначеності, який не піддається обробці ймовірнісними методами.

Розглянемо поняття ланцюга зв'язку, який відображає той факт, що два симплекси можуть і не мати спільної грані, але можуть бути зв'язані за

допомогою послідовності проміжних симплексів. Ураховуючи наведене вище, поняття q-зв'язку може бути визначено наступним чином.

Вважається, що задана пара симплексів σ_p, $\sigma_r \in K$ зв'язана у ланцюг, коли існує скінчена послідовність симплексів $\sigma_{a1}, \sigma_{a2}, \ldots, \sigma_{ah}$ така, що:

- σ_{a1}– грань симплекса σp;
- σ_{a2}– грань симплекса σr;
- σ_{a1}та σ_{ah}– з'єднанні спільною гранню, наприклад, σ_{bi}, для b_{ii}= 1, ... , (h − 1).

Вважатимемо, що цей ланцюг зв'язку є q-зв'язком, якщо q є найменшим із цілих чисел $\{a_1, b_1, b_2, \ldots, b_{h1}, a_h\}$.

Отже, якщо два симплекси мають q+1 спільні вершини (спільні q-мірні симплекси), то вони є q-зв'язаними. Алгоритм знаходження значень q для спільних граней усіх пар симплексів у K та алгоритм одержання значень використовує матрицю інцидентності δ, що визначає K, наведений у цій роботі [14].

Вивчення структурно складних систем вимагає дослідження як на глобальному рівні з позицій структури як єдиного цілого, так і на локальних рівнях з позицій окремих підсистем та елементів. Для вирішення завдань аналізу зв'язності систем видається корисним застосовувати апарат алгебри топології, що дозволяє проводити аналіз структури як складного багатовимірного геометричного світу – симплеціального комплексу та використовувати інструмент симплеціального аналізу зв'язності [15, 16].

Як відомо, в симплеціальному аналізі система розглядається у вигляді відносини між елементами множин – вершин V і заданого сімейства непустих підмножин цих вершин – симплеціальних комплексів. Структура системи служить підставою для геометричного і алгебраїчного її подання як симплеціального комплексу K, утвореного множиною вершин і відповідних їм симплексів. Для їх побудови може бути використана структура системи, заданої у вигляді когнітивної карти. Будь-яке відношення у системі представляється таким чином, що множина, яка співвідноситься з конкретним

елементом трактується як симплекс – геометрична розмірність якого визначається числом дуг, що з'єднують вершини в симплексі через змінну. Симплекси можуть визначатися як по рядках (X), так і по стовпчиках (Y) матриці відносин графа, відповідно, можуть бути побудовані два комплекси.

Таким чином, симплеціальний комплекс вибудовується шляхом розбиття деякого простору, заданого, наприклад, графом G на підмножини. Оскільки симплеціальний комплекс – це сімейство симплексів, з'єднаних за допомогою загальних граней (в тому числі, загальною вершиною – точкою), то характеристикою зв'язності може слугувати розмірність межі, яка дорівнює двом симплексам. Оскільки комплекс функціонує як ціле, то для аналізу зв'язності використовується поняття «ланцюг зв'язку» – q-зв'язність. Ланцюг зв'язку відображає можливість того, що два симплекса, безпосередньо не маючи загальної межі, можуть бути пов'язані за допомогою послідовності проміжних симплексів.

На можливостях симплеціального аналізу ґрунтуються формалізовані правила обґрунтування вибору цільових і вершин, визначення стійкості систем, які характеризуються тими чи іншими симплеціальними комплексами, умовами структурної стійкості систем [17].

Використання симплеціального аналізу можливе при мінімальній апріорної інформації щодо досліджуваних об'єктів і явищ [18].

Сьогодні різні математичні методи широко використовуються у всіх сферах науки і техніки. Особливо актуальні вони при дослідженні об'єктів складної структури.

Симплеціальний комплекс є топологічною структурою, тому він краще ніж графи описує взаємозв'язок між частинами системи та її елементами. Також в цьому контексті використовується поняття q-зв'язності, тобто рівень зв'язності між симплексами у комплексі. На кожному рівні такої зв'язності симлеціальний комплекс можна описати як сукупність ланцюгів, тобто як граф, вершинами якого є симплекси, а ребра – зв'язки розмірності не менше ніж даний рівень зв'язності (який розглядається). Такі графи ще називають

локальними картами [19], бо вони відображають внутрішню структуру ланцюгів.

Визначення 1. Локальною картою симплеціального комплексу називається граф бінарного відношення q-примикання, вершинами якого є симплекси розмірності k>q, а ребра відповідають q-зв'язку між ними.

Визначення 2. Q-примиканням називається бінарне відношення між симплексами в симплеціальному комплексі, яке виникає при перерізі двох симплексів, і розмірність якого більше або дорівнює «q» [20].

Визначення 3. Q-зв'язком називається бінарне відношення, яке виникає при транзитивному замиканні q-примикання у симлеціальному комплексі [20].

На основі наслідування, за включенням ланцюгів суміжних рівнів зв'язності, виникає можливість побудови відповідного дерева [1]. Вершинами Q-дерева є ланцюги із симплексів, які є зв'язними на певному рівні зв'язності, а рівні глибини у дерева і є ті самі q-рівні зв'язності. Тобто структурний аналіз складної системи має результатом структурне дерево та локальні карти відповідного комплексу.

Структурний вектор Аткіна та ексцентриситети симплексів є лише не значною частиною повної інформації про структуру системи, заданої відповідним чином. Вище зазначений метод дозволяє кількісно оцінювати сукупність зв'язків між симплексами, які формують ланцюги в комплексі, що є важливим для дослідження структури системи в цілому [21].

Об'єднані в симплекс вершини можна розглядати як єдину вершину в деякому масштабі представлення симлеціального комплексу, і це створює можливості для більш ефективної (масштабованої) обробки інформації, пов'язаної з системою.

Крім цього, в системах управління можуть виникати задачі, які пов'язані з окремими підсистемами, коли доцільно працювати лише з певними симплексами, не впливаючи на комплекс в цілому, тобто зберігаючи їх зовнішні зв'язки. Тому необхідно мати навички не лише декомпозувати

систему (що і дозволяє зробити Q-аналіз), але і синтезувати її до первинного стану за потребою.

Також, виникають задачі управління, коли необхідно впливати не на всю систему в цілому, а лише на окремі підсистеми (симплекси), зберігаючи при цьому їх зовнішні зв'язки. Крім цього, необхідно мати навички для того, щоб корегувати систему в цілому, адже з часом можуть відбуватися зовнішні зміни або змінюватися вимоги користувачів. Обернена задача дає можливість відновлювати систему за наявності обмеженого набору даних, й водночас, синтезувати систему за заданими параметрами. Метод опису системи, як топологічного комплексу, одночасно можна перевести в терміни мережевої структури та описувати складні зв'язки за допомогою гіперграфів [107].

Для кожної розмірності q комплексу K визначимо ціле число Qq як число різних класів еквівалентності, де кожен клас еквівалентності складається з q-зв'язаних симплексів. Цей вектор з Qq є основою для прикладу, що ілюструє спрощення, яке може бути досягнуто шляхом усунення зайвих підказок у тій самій еквівалентності класів симплексів. Перший структурний вектор Q потім описує структуру симплеціальної зв'язності, Q = (Q(dim K), Q(dim K - l) , ... , Q0). Структурний вектор Q, який є безпосереднім результат Q-аналізу, може бути використаний для отримання додаткового розуміння взаємозв'язку між діагностичними підказками та діагностичними категоріями [22].

Ексцентриситет симплексу. Оскільки індивідуальні властивості симплексів можуть мати важливе значення для вирішення поставленої задачі, необхідно визначити міру інтегрованості кожного окремого симплексу в структурі всього комплексу системи.

Для цього вводиться поняття ексцентриситету, яке відображає ступінь ізоляції симплексів один від одного. Це поняття відображає як відносну важливість даного симплексу для комплексу в цілому (через його розмірність), так і його значимість як сполучної ланки (через максимальне число його вершин, що належать також будь-якому іншому симплексу). Іншими словами,

ексцентриситет дозволяє побачити і оцінити, наскільки «щільно» кожен симплекс вкладений у комплекс.

Ексцентриситет симплексу σ визначається за формулою (1.19), яка відображає ступінь ізоляції симплексів один від одного [19]:

$$Ecc(\sigma) = \frac{\hat{q} - q^{\check{}}}{q^{\check{}} + 1}, \quad (1.19)$$

де верхнє значення $\hat{q}$ є значення розмірності відповідного симплексу P_i, тобто $\hat{q}$ = dim P_i у K. Можна констатувати, що це значення чисельно дорівнює рівню зв'язності, на якому цей симплекс вперше з'являється в складі симплеціального комплексу;

нижнє значення $q^{\check{}}$ є найбільшим значенням q, при якому P_i стає зв'язаним із будь-яким окремим P_j. Іншими словами, це кількість вершин, принаймні одна, які є спільними для даного симплексу та інших окремих симплексів.

З означення випливає, що $\hat{q} \geq q^{\check{}}$.

Чисельник виразу дає інформацію про «абсолютний» ексцентриситет симплексу, а знаменник нормує це значення до «відносного». Порівнюючи значення ексцентриситетів множини X та Y, можна відзначити, чи ізольований кожний симплекс комплексу від інших, чи існують серед множин елементи, відносно стійкі до змін всередині множини цих елементів.

Найменшим значенням, яке може приймати ексцентриситет, є $Ecc(\sigma) = 0$. Це означає, що симплекс є q-суміжним з симплексом такої ж самої, але більшої розмірності, тобто на рівні цієї розмірності відповідний симплекс є повністю «вбудованим» в симплеціальний комплекс і не має своїх унікальних вершин.

Якщо симплекс повністю відділений від інших елементів комплексу навіть на рівні зв'язності $q = 0$, то вважається, що він зв'язаний з іншими симплексами на рівні $q = -1$. Тоді його ексцентриситет дорівнюватиме нескінченності.

Нижче наводимо пов’язані визначення:

n-мірним остовом комплексу називається підкомплекс, який утворений усіма його симплексами розмірності не більше n.

Розмірність симплеціального комплексу визначається як максимальна розмірність його симплексів. Припустимо, що K є симпліціальний комплекс, і, припустимо, що S - деякий набір симплексів K.

Замикання *S* (позначається Cl(S)) є найменший підкомплекс в *K*, що містить кожен симплекс з *S*. Замикання $\underline{S}$ може бути отримано шляхом додавання до *S* усіх граней всіх симплексів з *S* (рисунок 1.11).

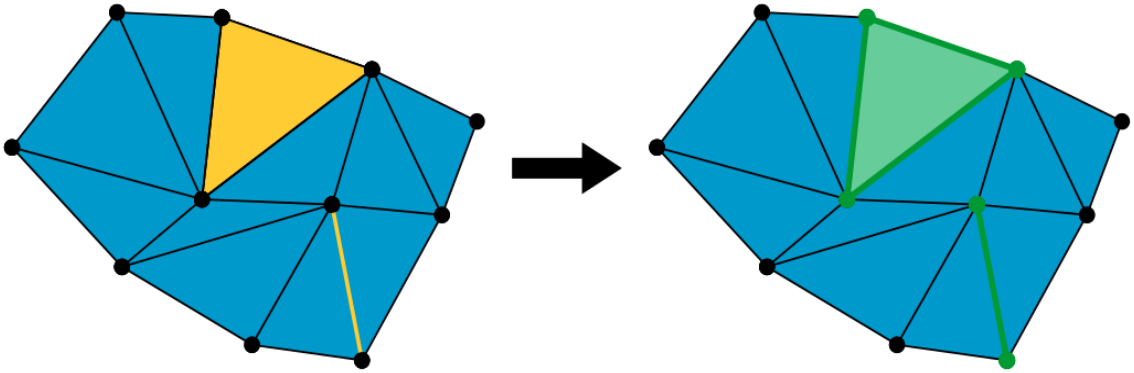


Рисунок 1.11 – Два симплекси та їх замикання [23]

Зірка від *S* (позначається St(S)) – об’єднання зірок всіх симплексів в *S*. Для одного симплексу *S* зірка *S* – це набір симплексів, що мають *S* своєю гранню. (Зірка – *S*, як правило, не є симплеціальним комплексом) (рисунок 1.12).

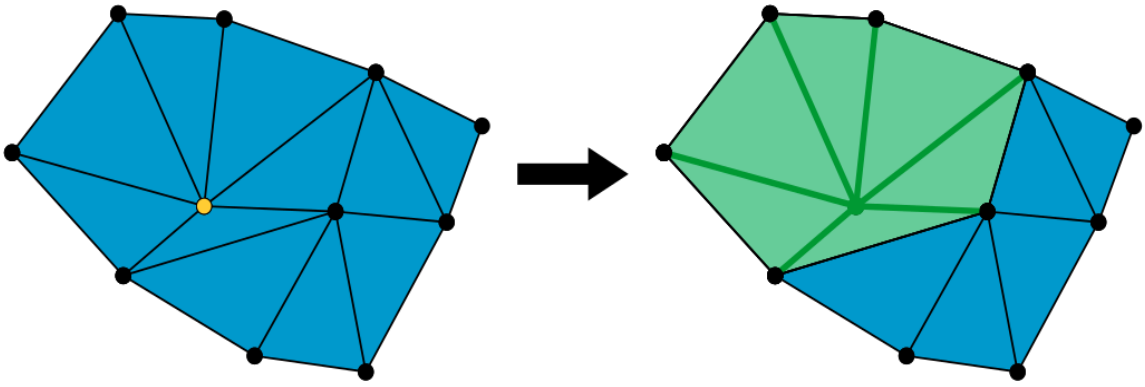


Рисунок 1.12 – Вершина та її зірка [23]

Лінк (зв'язок) S (позначається Lk(*S*)) може бути визначений як Lk(S)=Cl(St(*S*)\St(Cl(*S*).

Це підкомплекс, утворений усіма симплексами, що входять до симплексів більшої розмірності разом із симплексом *S*, але не мають граней з *S* [23] (рисунок 1.13).

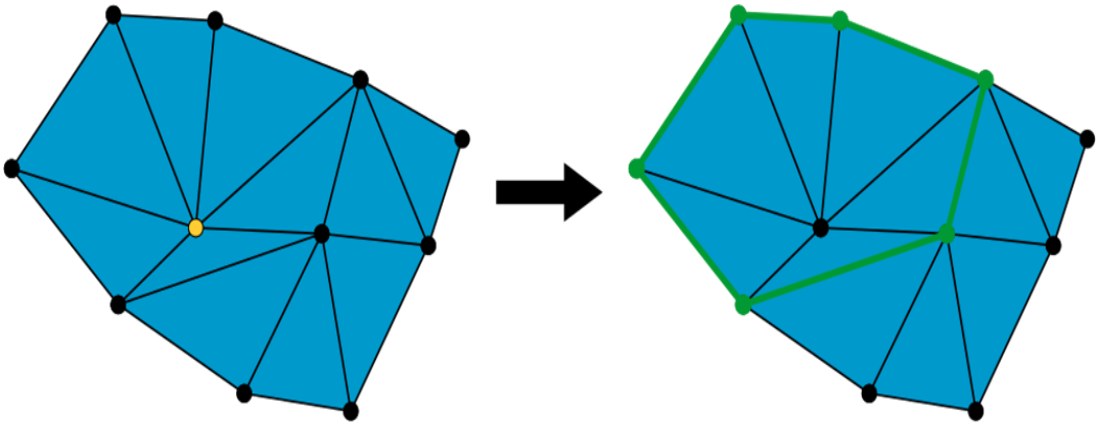


Рисунок 1.13 – Вершина та її лінк (зв'язок) [23]

Всі ці поняття тісно пов’язані з структурними особливостями системи. Зміна будь-якої частини підсистеми порушує взаєморозташування зірки, остова та лінка (зв’язка), що, у свою чергу, може призвести до виникнення додаткових уразливостей та загроз. Тому зазначені вище опорні особливості дозволяють не відслідковувати кожен симплексом окремо, а за певною структурною одиницею. Це дуже зручно, коли в системі занадто багато елементів.

1.4.3 Переваги та недоліки класичного Q-аналізу

Q-аналіз є математичною мовою, а не статистичним методом, і не пов’язаний з теорією ймовірностей. Це дає Q-аналізу потужну описову перевагу при вирішенні поставлених завдань, для яких статистичні методи є недоречними або відсутні. У будь-якому випадку, Q-аналіз не включає статистичної обробки взагалі. При цьому, Р. Х. Аткін визначив обставини, за яких теорія ймовірності може бути застосована [24].

Q-аналіз покладається на однозначне визначення наборів симплексів і використання зв’язків між ними. Останнє дозволяє зазначеному методу бути «дружнім» до вхідних даних. Недостатнє використання таких понять, як теорія, гіпотеза чи моделі в Q-аналізі вимагає особливої уваги до формування вхідних даних. Це може призвести до того, що Q-аналіз може вважатися антинауковим.

Різними вченими також наводяться приклади, як Q-аналіз застосовується до вирішення багатокритеріальної задачі прийняття рішень із застосуванням методу, що називається багатокритеріальним Q-аналізом [22]. У наукових роботах також обговорюються переваги та обмеження Q-аналізу, а також пропозиції щодо його майбутнього використання.

Недоліками Q аналізу можна вважати наступні.

1. Отримуються лише якісні показники співвідношень, на відміну від статистичного аналізу, проте статистичний аналіз вимагатиме однотипних реплікацій наборів даних.

2. Математична теорія технічно є не простою, однак, глибоке розуміння цієї теорії не суттєве для застосування та правильної інтерпретації результатів.

3. Є багато показників, які можуть бути використані, тому повинні бути прийняті метрики для подальшого порівняння результатів.

4. Інтерпретація результатів не завжди є простою.

Основні переваги використання Q-аналізу:

1. Це простий у використанні метод, що вимагає лише арифметичних типів обчислень.

2. Метод гнучкий, тобто немає проблем при зміні q-рівнів або визначень предметних асоціацій.

3. Забезпечує визначення як на прямих, так і опосередкованих показниках (наприклад, рівні q-зв’язків, ексцентриситет, класи еквівалентності відношень зв’язків та елементи структурного вектора).

4. Може бути використаний у методах багатокритеріального прийняття рішень, а також для вирішення багатьох інших проблем, пов’язаних з динамічним аналізом структури бінарного зв’язку.

Історично Q-аналіз застосовувався в широкому спектрі застосувань, включаючи такі різноманітні сфери, як шахи [25], футбол [26], екосистеми озер [27], транспорт [28], ринкові системи [29], економічні системи [30], підприємницькі мережі [31], великі дані та складність [32] і навіть моделі переміщення розташування торгових центрів [33]. Проте, серед найбільш помітних застосувань, які мали значний вплив на розвиток цього напрямку дослідження, були дослідження з аналізу структури та функціонування міст [25], складності структури телевізійних програм [34], розташування об’єктів сільського господарства та комунікації [35].

У своїй роботі з аналізу міст Аткін Р. Х. визнав обмеження двовимірної карти для отримання та точного опису фізичних властивостей та функціонування міста чи громади. Внаслідок цього, в дослідженні було запропоновано охопити територію міста набором ромбів (тобто одиниць площі) довільного розміру та форми, щоб урахувати важливі об’єкти міста (наприклад, торгові центри, житлову нерухомість, зручності тощо). Водночас, було також наголошено, що ці розподілені області повинні бути достатньо малими, щоб у разі потреби об’єднуватися в більш великі за площею. Асоціація між частинами та рисами міста створила основу для міської громади в окремому районі. Аналіз зв’язності структури міської громади продемонстрував, що Q-аналіз можна застосовувати як інструмент прийняття рішень для міського планування, оскільки він може сприяти розвитку оптимально збалансованої та функціонуючої громади, включаючи зовнішній вигляд та естетику міста [25]. Подібні дослідження в наведеній вище сфері також виявили корисність Q-аналізу для інтерпретації складних структур даних і кращого розуміння міських систем [35].

Дослідження у сфері телебачення чітко визначило труднощі наявності визначеної структури телевізійних програм на різних рівнях узагальнення.

Причина визначення такої складної структури мала на меті сприяти розвитку науки та політики у цій галузі досліджень. За результатами проведеного дослідження було визначено чітке розмежування змісту програми та її категорійного розташування (наприклад, освіта, розваги, різне). Такі відображення були визначені як ієрархічні, що означає, що симплекс заднього полотна на рівні N можна було відобразити із симплексом трафіку на будь-якому ієрархічному рівні, наприклад, N+2 [34]. Ці та інші напрацювання цього дослідження визначили цінну теоретичну базу для вивчення інших великомасштабних ієрархічних структур і належним чином врахували їх описові компоненти та особливості.

Ураховуємо також особливості застосування Q-аналізу, наведені ще у одному великому дослідженням стосовно галузі сільського господарства та комунікації. Результати цього дослідження також мають значний інтерес і практичну цінність у контексті цієї роботи. Як заключне зауваження, слід визнати, що теорія і методологія Q-аналізу продовжують еволюціонувати, рухаючись у напрямку більш чітких і помітних теоретичних основ для задоволення потреб в організації, управлінні та аналізі складних даних. Останнє призвело до розвитку та теоретичного формалізму гіпермереж, які покликані забезпечити інструменти інтерпретації для багаторівневих систем заднього руху, однозначного визначення таких багаторівневих систем і реляційного відображення, а також всебічного використання симплексів, симплеціальних комплексів та Q-аналізу.

Значний прогрес у цій сфері досягнуто Джонсоном Д. Х., яким узагальнено наявні напрацювання застосування теорії і методології Q-аналізу у роботі про мережеві структури в складних системах [36,37]. Важливо також зазначити, що існують інші та прикладні напрямки використання теорії Q-аналізу, які не були розглянуті в цій дисертації, оскільки вони виходять за рамки дослідження, зокрема застосування таких понять, як ексцентриситет або динаміка.

Висновки до розділу 1

Перший розділ присвячений огляду літератури з напряму дослідження дисертації. Описано основні методи та їх застосування в області аналізу загроз та вразливостей кіберсистем, оцінювання ризиків, аналізу структури складних систем, Q-аналізу.

У розділі висвітлено актуальність аналізу та застосування методів виявлення та оцінки кібервразливостей та пов'язаних з ними загроз. Проаналізовано основні підходи до оцінювання ризику в залежності від допустимого рівня втрат.

Здійснено порівняльний аналіз сучасних підходів до аналізу складних кіберсистем. Сформовано набір терміні для проведення подальшого дослідження. Сформульоване поняття «складності» як наукової теорії, яка стверджує, що деякі системи демонструють поведінкові явища, які абсолютно неможливо пояснити будь-яким звичайним аналізом складових частин системи.

Розглянуто методологію аналізу життєвого циклу вразливостей, їх виявлення у кіберсистемах. Запропонований підхід дозволяє аналізувати, прогнозувати та реагувати на вразливості, планувати запобіжні заходи для попередження їх виникнення – тобто керування вразливостями.

Проаналізовано підходи до аналізу структури систем, ключовим методом дослідження визначено Q-аналіз. Наведено принципи та методологію класичного Q-аналізу, який буде уточнено та розвинуто у ході даного дослідження.

Продемонстровано, що сучасні існуючи методи аналізу ризиків у кіберсистемах не дозволяють урахувати їх структурну складність та оцінити рівень збитків при сумісних реалізаціях кіберінцидентів. Розроблено та обґрунтовано відповідні методи оцінювання ризиків, на основі яких можна розробляти системи підтримки прийняття рішень щодо застосування заходів зі зменшення ризиків.

РОЗДІЛ 2

СТРУКТУРНИЙ АНАЛІЗ ЗАГРОЗ ТА ВРАЗЛИВОСТЕЙ КІБЕРСИСТЕМ

2.1 Алгоритми знаходження структурних характеристик кіберсистем

Найчастіше кібератаки відбуваються в тих компаніях або організаціях, які володіють так званою «чутливою» або конфіденційною інформацією [78]. Адже це може негативно позначитися на репутації організації через витік зазначеної інформації, порушення законодавство про захист персональних даних тощо.

Звичайно, інформація про такі інциденти частіше оприлюднюється стосовно організацій державного сектору, але і комерційні компаній достатньо вразливі до таких атак. Однак приватні установи намагаються приховати такі випадки для того, щоб зберегти свою репутацію. Статистичні дані 2017 року свідчать про те, що комерційні компанії в середньому втратили близько 200 тис. доларів США на рік унаслідок несанкціонованого втручання [98].

Найчастіше загрозу для несанкціонованого втручання до інформаційних ресурсів компанії становлять її ж працівники. Іноді це спеціально завербовані люди, але більшість випадків кібератак спровоковані недостатньо обізнаними працівниками, які погано розуміються на інформаційних технологіях або занадто довірливі. Для запобігання цьому необхідно підвищувати кваліфікацію працівників у сфері кібернетичного захисту за допомогою роз’яснень щодо можливих способів проникнення кіберзлочинців в інформаційні системи та методів і механізмів захисту від цього. Для підвищення рівня відповідальності працівників за ті чи інші дії, що можуть або привели до кібератаки доцільно впроваджувати відповідні правила та регламенти роботи.

Окрім підвищення рівня обізнаності працівників, у кожної компанії має бути розроблена так звана «політика кібербезпеки», тобто певний статут, який

регулює як і яким програмним забезпеченням може користуватися працівник на робочому комп'ютері (обладнані). Також, використання персональних девайсів, має відстежуватися та аналізуватися системою моніторингу на предмет вірогідності використання зловмисного програмного забезпечення. Звичайно, такі статути не мають обмежувати права людини. Але все, що може зашкодити компанії, повинно бути прописано та хоча б у рекомендаційному порядку донесено до працівників. Однією з рекомендацій може бути обмеження часу та запровадження умов використання персональних девайсів в офісі компанії.

Для запровадження політики кібербезпеки необхідно видати розпорядчий документ, у якому прописані всі положення стосовно правил трудового розпорядку та кібернетичної гігієни у середині компанії, ознайомлення з яким працівники затверджують підписом. Недотримання вимог має передбачати певне покарання у залежності від ступеню порушення та наслідків, які спричинила зловмисна або безвідповідальна поведінка робітника. Окрім самого працівника, відповідальність має нести його керівник та інші співробітники, які причетні до моніторингу кібербезпеки. Кожний випадок порушення політики інформаційного та кібернетичного захисту має бути розслідуваний. У разі, коли виявлені незначні порушення – вимагається проведення роз'яснювальної роботи, а у разі серйозних провин – штраф чи звільнення.

Для проведення аналізу функціонування інформаційної системи, необхідно з'ясувати, які кіберзагрози характерні для даної сфери діяльності. Наприклад, якщо система включає бізнес процеси, інформаційні технології тощо, тоді найчастіше виникають загрози таких типів, як фішінг, неавторизований доступ тощо. Для їх попередження потрібно використовувати різні схеми запобігання, але найголовніше – це обізнаність працівників.

У різних компаніях необхідність щодо забезпечення кіберзахисту має різну ступінь важливості, але загалом існує достатньо інструментів для

здійснення ідентифікації загроз та спроб зловмисного входу в систему. Щоб зрозуміти, як різні вразливості впливають на можливості кібератак необхідно використовувати певне програмне забезпечення та відстежувати дії, які відбуваються в системі. Кожна система має складну структуру. Інколи відстежити взаємопов'язаність різних елементів системи може бути занадто трудомісткою задачею. Особливо, коли систему не можна представити у формі звичайного графа або гіперграфа. У цьому випадку доцільно застосовувати Q-аналіз, основні дослідження наведені в [5-12].

У теорії Q-аналізу елементарними частинами є симплекси, тобто більш складна структура ніж вершини та ребра. Це дає змогу досліджувати деякі підсистеми, що мають більш просту будову, але також мають такі ж самі характеристики та елементарні частини, як і в єдиному цілому. Такий підхід, дозволяє зрозуміти, що саме ця елементарна частина є неподільною, а, отже, будь-яка вразливість елемента з симплексу руйнує його в цілому при реалізації атаки.

Інше питання – це взаємозалежність між симплексами. Для реальної системи – це зв'язок між підсистемами або пов'язаними системами. Ці зв'язки мають особливість у порівнянні зі зв'язками у графах. Вони показують як сильно в/будовані різні елементи один в одного. Для кіберзахисту це дає розуміння того, як вразливості однієї системи впливають на інші. Після побудови симлеціального комплексу на основі системи можна побудувати відповідний комплекс для вразливостей. Здійснення аналізу структурного дерева і локальних карт дозволяє внести корективи у систему та по можливості зменшити ступінь зв'язності. Особливо актуально це для критичних підсистем, де зберігається конфіденційна інформація.

У кібербезпеці використовуються різні метрики для оцінки якості захисту системи. Щоб зрозуміти, які саме метрики потрібні, необхідно провести аналіз потоку даних, журналів безпеки тощо. Найцікавіше та найскладніше в аналізі системи – це знайти ті зв'язки, які не випливають зі звичайного поняття зв'язків, яке використовується в теорії графів та

пов’язаними з ними мережими структурами. Це є предметною сферою застосування Q-аналізу. Виходячи з цього, головна мета його використання якраз полягає в тому, щоб віднайти «приховані» зв’язки.

Пошук відповідей на запитання: яким чином і за допомогою яких метрик можна віднайти приховані зв’язки та спровоковані ними загрози для системи є основним завданням даного дисертаційного дослідження.

Спочатку потрібно зібрати всі необхідні дані. У разі, коли є доступ до моделі системи, хоча б у вигляді графу, то це значно полегшує роботу та подальший аналіз, оскільки маємо розроблену методологію переходу від графу до симлеціального комплексу. У разі відсутності або обмеженості таких даних, потрібно побудувати граф або відразу моделювати систему в понятті симплексів та зв’язків між ними. Для цього потрібно виявити елементарні частини системи, типи зв’язків між ними та бачення різних спеціалістів, що працюють з системою, як саме використовуються певні елементи. На основі цих даних та методології побудови симплеціального комплексу можемо побудувати модель для системи.

У наступних підрозділах будуть розглядатися алгоритми побудови симлеціального комплексу та побудови та аналізу систем за допомогою Q-аналізу.

Наведемо загальну методологію збору необхідних даних [1,2]. Розглянемо декілька варіантів представлення вхідних даних. Припустимо, що загальна модель системи – невідома, але завжди можна визначити чи мають між собою зв’язок її елементи, передбачивши різні комбінації.

Для побудови симплеціального комплексу потрібно визначити, які існують попарні, тернарні та іншого рівня зв’язки між елементами системи. Це можна зробити, маючи інформацію стосовно структури системи або застосовуючи певну методологію опитування у експертів чи розробників системи.

У випадку дослідження вразливостей системи основними об’єктами дослідження є зв’язок та сумісність виникнення їх у системі, а також

взаємозалежність загроз від певних комбінацій їх одночасного виникнення в системі. Припустимо, що задача полягає у відновлені структури системи вразливостей. У цьому випадку опитування експертів проводиться у напряму виявлення різного роду сумісностей між окремими вразливостями. Всі ці зв'язки інтерпретуються за допомогою термінології симплеціальних комплексів. Тобто для бінарних сумісностей виникають ребра, для тернарних – грані тощо. Таким чином формується симплеціальний комплекс, який з високою точністю відображає структуру системи вразливостей кібернетичної системи. Такий підхід відрізняється від понять гіперграфів та мереживих структур, адже висвітлює «прихований» вплив між вузлами.

Інший випадок більш легкий з точки зору формальної побудови. Якщо наочно існує матриця інцидентності залежності вразливості та загроз, то можна використовувати алгоритми наведені нижче. Такий підхід більш структурований та краще обраховується за допомогою комп'ютера. Але зазвичай такі матриці або знаходяться емпіричним шляхом, або мають гіпотетичний характер. Надійність такого підходу є не достатньою, але він є доступним у застосуванні, що, безперечно, дозволяє полегшити проведення аналізу та обрахунків.

Основним показником складної структури зв'язків є ідентифікація q-зв'язності. Для того, щоб її віднайти, необхідна матриця інцидентності, тобто звичайна матриця зв'язків для графу Δ. Рівні q-зв'язності визначають класи еквівалентності Q_q.

Множини, що відповідають за елементи в системі і використовують за структурну одиницю симплекс, мають відповідні позначення X з розмірністю m та Y з розмірністю n. Матриця інцидентності відповідно має розмір m×n, що складається з нулів та одиниці. Добуток прямої матиці Δ на транспоновану Δ^T, дає нам число, що відповідає скалярному добутку рядків і та стовпців j, одиниць, що відповідає значенню q+1, q – розмірність сусідніх граней симплексів σ_p та σ_r, заданих рядками i та j. Також це число показує скільки в одних і тих самих місцях (у рядках i та стовбцях j) є зв'язків, а отже і одиниць.

Алгоритм знаходження q-спільних граней для пар з Y-симплексів у комплексі K_Y(X; λ) полягає в наступному (рисунок 2.1).

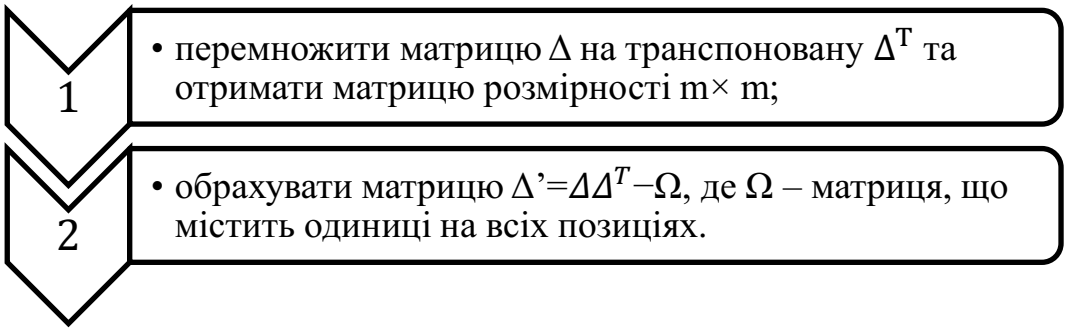


Рисунок 2.1 – Схема алгоритму побудови матриці симплеціального комплексу

Отримуємо матрицю, яка показує рівень зв'язності, так званої q-зв'язності між симплексами, а діагональні елементи відповідають розмірності самих симплексів, що присутні в комплексі.

Q-зв'язність дає відношення еквівалентності на комплексі. Тому задача вивчення структури комплексу, його зв'язності полягає в знаходженні цих класів. Внаслідок цього кожному рівню q-зв'язності відповідає певний клас еквівалентності Q_q.

Наступним кроком є знаходження симплексів, що відповідають певному класу. Для визначення цього будують A^k – матриці q-зв'язків $k = \overline{0,n}$, де n – кількість класів еквівалентності.

Також необхідно зрозуміти, наскільки сильно та структурно складно взаємопов'язані елементи симлеціального комплексу. Для подальшого знаходження конкретних симплексів у кожному класу еквівалентності, будуються матриці A^k q-зв'язків $k = \overline{0,n}$, де n – кількість класів еквівалентності. Відповідний алгоритм виглядає наступним чином.

Для всіх k:

$$A^k = \{a_{ij} = 1, \text{якщо } \Delta ij > k, \text{інакше: } a_{ij} = 0 \qquad (2.1)$$

Алгоритм знаходження симплексів для кожної матриці A^k:

1. Обираємо $a_{11}{}^k$, знаходимо всі недіагональні елементи строки 1.

2. Додаємо їх до симплексу з позначкою рівня зв'язку.

3. Переходимо до тих строк, для яких номер співпадає з j першої строки.

4. Для кожної строки, якщо існують такі ненульові елементи для яких j>i, додаємо їх до симплексу і переходимо до тих строк як у п.2.

5. Після проходження всієї матриці видаляємо стовбці та строки тих елементів, які були додані до поточного симплексу.

6. Продовжуємо алгоритм спочатку, поки матриця не виродиться.

7. Всі ітерації повторюємо для кожної матриці A^k.

Побудова структурного вектора

Структурний вектор відображає кількість класів еквівалентності та рівень убудованості симплексів кожного рівня q-зв’язності Q_q. Він виглядає таким чином:

структурний вектор зв’язності комплексу Q = (Q_n, Q_{n-1} ... Q_1, Q_0), де Q_n= $Q_{dim\,K}$.

Після отримання симплексів кожної розмірності за допомогою попереднього алгоритму будуємо транзитивне замикання для відношення симплеціального комплексу.

Транзитивним замиканням відношення R називається таке бінарне відношення R' при якому xR'y тоді і тільки тоді, коли існує ланцюжок елементів з X, наведений нижче:

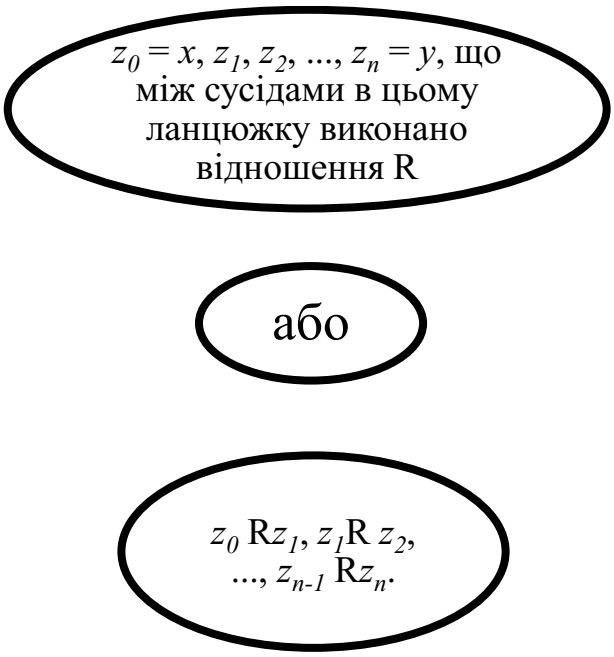


Рисунок 2.2 – Схема побудови транзитивного замикання ланцюгів симплексів

Для побудови транзитивного замикання для матриць q-зв'язності доцільно застосовувати алгоритм Уоршалла [96] для звичайних матриць інцидентності, узявши матриці зв'язності з попереднього алгоритму. На виході алгоритму отримуємо ланцюги зв'язних симплексів на кожному рівні q. Далі рахуємо кількість ланцюгів та отримуємо структурний вектор. Цей вектор дає певне сукупне уявлення щодо складності структури систем та зв'язків між елементами.

Пошук «нащадків»

Для відслідковування того, які підсистеми найбільше взаємопов'язані, за допомогою методології Q-аналізу, вводимо похідне поняття «нащадків». Це поняття відображає, які з симплексів включають в себе елементи із найсильнішим зв'язком. Сильна q-зв'язність певного ланцюга відображається великим числом у структурному векторі, а, отже, великою кількістю нащадків.

Для того, щоб відслідкувати нащадків, використовуємо матриці q-зв'язку. Починаючи з першого рівня, на кожній ітерації позначаємо відповідність: який саме ланцюг породив той чи інший наслідковий ланцюг.

Після цього, рахуємо кількість ланцюгів кожного рівня для кожного симплекса.

Процедура обрахунку нащадків наведена нижче (рисунок 2.3):

1. Для всіх i==$\overline{0, \mathrm{m}}$, де m – розмірність матриці зв'язку та для всіх k=$\overline{0, \mathrm{n}}$, де n – розмірність структурного вектора.

2. Вибираємо перший елемент матриці t_{ii} та знаходимо симпліціальний ланцюг, в який він входить.

3. Відмічаємо лічильником j=$\overline{0, d}$, де d – значення структурного вектора на кожному рівні, кожний елемент даного ланцюга.

4. Операцію проводимо для всіх ланцюгів симлеціального комплексу.

5. Переходимо до матриці k=k+1.

6. Переносимо відмітки з попередньої матриці.

7. Починаємо алгоритм з п. 2 [1].

Цей алгоритм використовується, зокрема для побудови структурного дерева. В отриманих матрицях B^k, k є позначкою елемента, якого сиплексу він відноситься. Далі необхідно видалити вектори, що повторюються з матриць B^k. Підрахувавши кількість елементів у тих векторах, що залишились, отримуємо кількість нащадків.

Побудова структурного дерева

В класичному представлені Q-аналізу для того, щоб отримати інформацію про цілісність структури системи (симплеціального комплексу) достатньо отримати структурний вектор. Але таке представлення не відображає структуру комплексу на кожному рівні q-зв'язності.

,

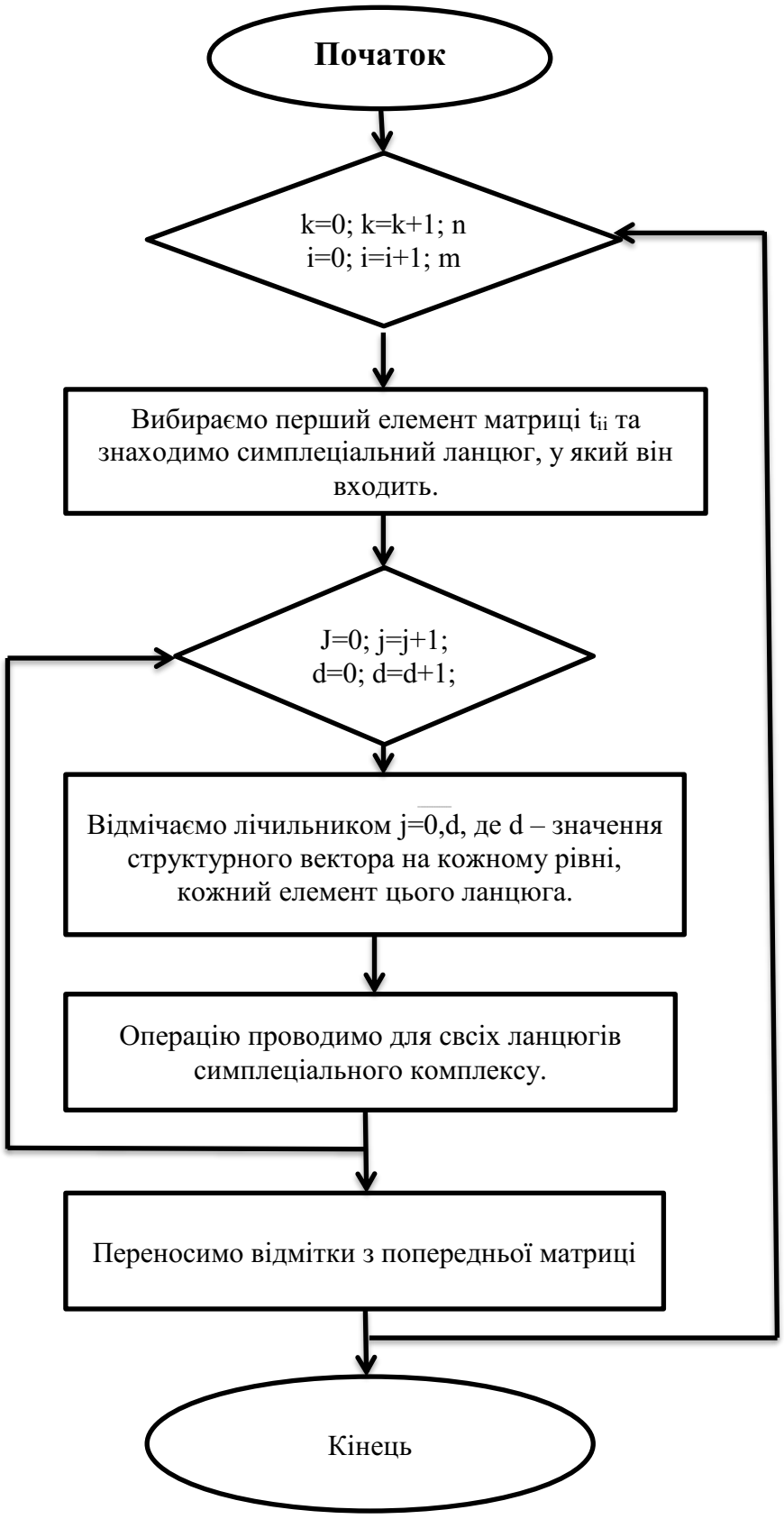


Рисунок 2.3 – Схема алгоритму пошуку нащадків

Більш наочно виглядає структура у вигляді дерева. Структурне дерево або Q-дерево визначається з ланцюгів симплексів для кожного рівня q-зв'язності. Визначимо алгоритм побудови Q-дерева. Для цього кількість симплексів, що входять в структуру комплексу позначимо n. Використовуємо матриці q-розмірності, отримані вище. Діагональні елементи відповідають розмірності симплексу 1.

Алгоритм побудови Q-дерева наведений нижче (рисунок 2.4):

1. Формуємо корінь дерева, елементи якого означають зв'язність симплеціального комплексу на рівні q = -1.

2. Будуємо вузли-нащадки q_1, …, q_m для рівня зв'язності q = 0. Число m відповідає кількості незв'язних компонент на даному рівні зв'язності.

a. Формуємо вузол-нащадок q_1, аналізуючи, які симплекси входять до цього вузла. Автоматично до нього входить симплекс σ_p, де p = $\min_i a_{ii} \geq q$. Після цього, розглядаємо всі інші симплекси мірності не менше q: σ_{p+1}, σ_{p+2}, …, σ_{p+t}, $t \leq n-p$. Якщо розглянутий симплекс є зв'язним з симплексом σ_p (або з будь-яким тим, який вже увійшов до складу вузла q_1) на даному рівні зв'язності q (тобто σ_p,$p+j \geq q$, то включаємо симплекс σ_{p+j}до вузла q_1.

b. Якщо серед симплексів, які мають мірність не менше q, залишились такі, які не увійшли до складу вузла-нащадка σ_k, формуємо вузол-нащадок q_2, записуючи до нього один із симплексів із тих, що залишились (позначимо як σ_k), та приєднуємо до нього інші симлекси, які зв'язані з σ_k на рівні зв'язності q = 0.

c. Продовжуємо виділяти вузли-нащадки q_1., доки не включимо до складу різних вузлів всі симплекси, які мають розмірність не менше q + 1.

d. Якщо вузол q_1. складається лише з одного симплексу розмірності q, то вважаємо даний вузол листовим елементом дерева.

3. Продовжуємо аналогічно будувати вузли-нащадки q_1., …, q_m для рівнів зв'язності q≥0, виконуючи пункти a-d з кроку 2. Кожен вузол-нащадок формуємо виключно з симплексів, які входили до складу батьківського вузла.

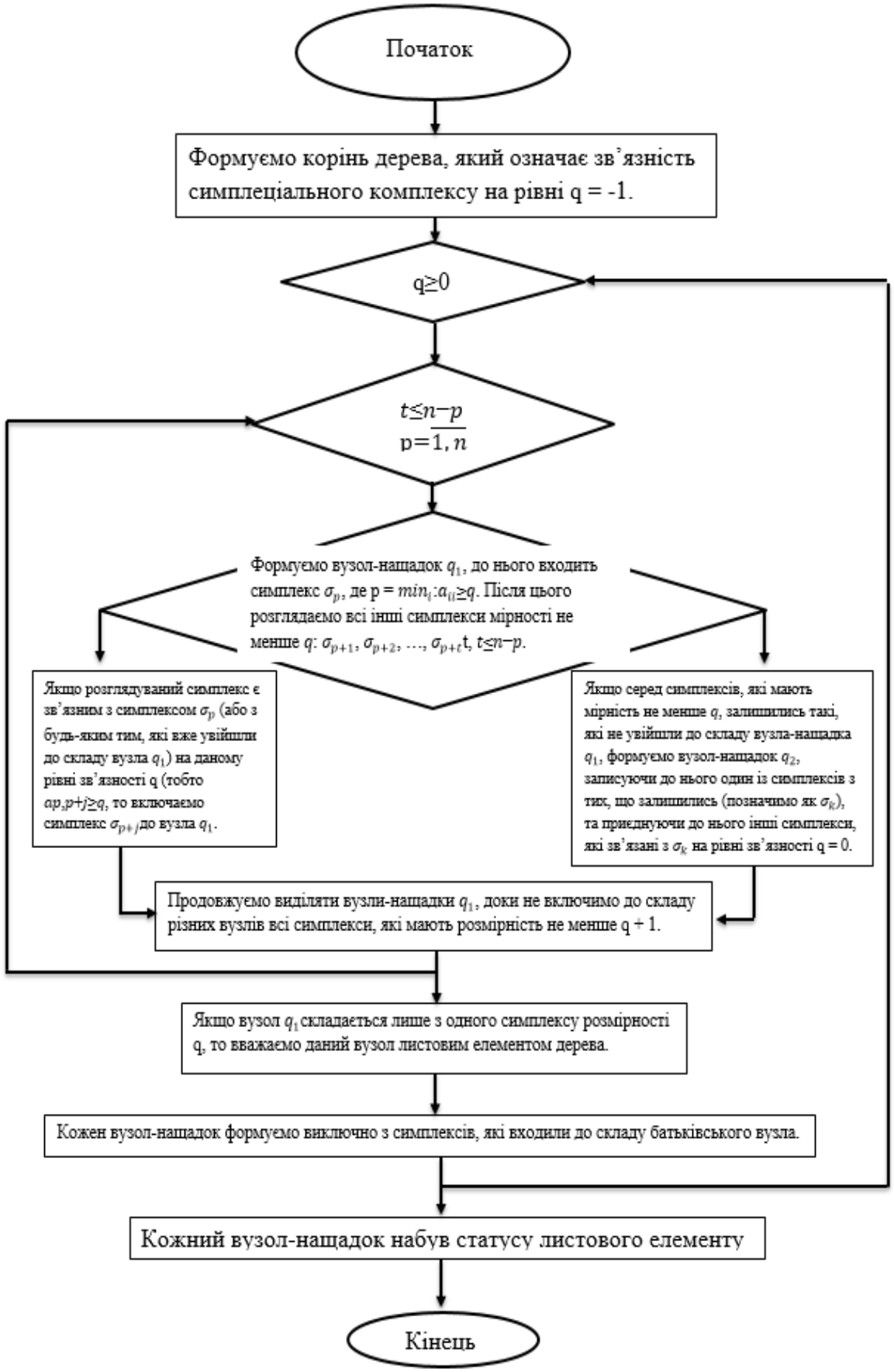


Рисунок 2.4 – Схема алгоритму побудови структурного дерева

4. Закінчуємо алгоритм, коли кожний вузол-нащадок набув статусу листового елементу [1].

Побудувавши Q-дерево, можемо відслідкувати на які симплекси розклеюється кожний ланцюг в симлеціальному комплексі, а, отже, з яких компонентів складається система. Можна також відслідкувати на якому рівні зв'язності той чи інший компонент зникає, а отже має певний рівень складності зв'язку.

Побудова локальних карт

Локальні карти відображають, як саме симплекси зв'язані між собою на кожному рівні q-зв'язності. Також ці карти надають інформацію: чи існують опосередковані зв'язки, і яка структура між зв'язаними напряму симплексами, а отже компонентами системи. Кожна локальна карта, що відповідає кожному рівню q-зв'язності, дає уявлення про взаємозалежність різних структурних компонент системи. Це дозволяє при проведенні подальшого аналізу використовувати цю інформацію для запобігання серйозних прогалин у відстеженні вразливостей у системі.

Процедура побудови симплеціального комплексу складається з таких етапів. Використовуємо визначені матриці А для кожного рівня q-зв'язності. Елемент матриці $a_{ij} = c, (c > 0)$, означає, що симплекси σ_i та σ_j поєднані c+1 спільними вершинами, тобто мають q-зв'язність розмірності c. Якщо, наприклад, c=1, це означає, що відповідні симплекси зв'язані ребром і мають 1-зв'зність. Випадок, коли c<0, свідчить про відсутність зв'язку між симплексами. Як зазначалося вище, діагональні елементи відповідають розмірності кожного симплексу. Загальну кількість симплексів у комплексі будемо позначати як n.

Якщо ж не має підготовленої структури інформаційної системи, тоді маємо побудувати симлеціальний комплекс на основі тих знань, які наявні. Побудувати ієрархію зв'язків та певну топологію на кожному з цих рівнів є не складною задачею. Наявні знання дозволяють побудувати або відновити

симплеціальний комплекс за допомогою наступного алгоритму [1], наведеного на рисунку 2.5.

Для того, щоб побудувати симплеціальний комплекс необхідно запустити алгоритм відновлення на основі методу синтезу. Для відновлення необхідно мати локальні карти та структурне дерева. В системі аналогом може бути топологія підсистем мережі та ієрархія зв'язків. У якості симплексів можуть виступати або окремі вузли, або нероздільні об'єднання серверів або комп'ютерів.

Проблемним питанням залишається те, як саме вірно враховувати під'єднання окремих частин. Тому для топології застосовано гіпотезу про існування ізоморфізму, який в структурі забезпечить правильне розташування симплексів. Ця гіпотеза базується на відношенні еквівалентності [2].

Позначимо множину вершин симплексу *C*. Ізоморфізм являє собою відображення множини самої в себе $f: C \to C$. Ізоморфізм f дає змогу перейменувати вершини в симплексі таким чином, щоб всі елементи системи, за який він відповідає мали правильну орієнтацію.

Гіпотеза. Для будь-яких двох симплеціальних комплексів, в яких співпадає структура (кількість вершин, симплексів та локальні карти), існує такий ізоморфізм $f: C \to C$, який перейменовує вершини в симплексі таким чином, що комплекси стають тотожними [2].

Така гіпотеза не є доказовою на даному рівні дослідження симлеціальних комплексів та графів, тому використовуємо як припущення.

Для побудови (синтезу) комплексу необхідно мати структурне дерево або вектор, а також локальні карти для кожного рівня.

Вхідні дані:

- Структурний вектор
- Локальні карти

Вихід алгоритму:

- Симлеціальний комплекс, ізоморфний вихідному.

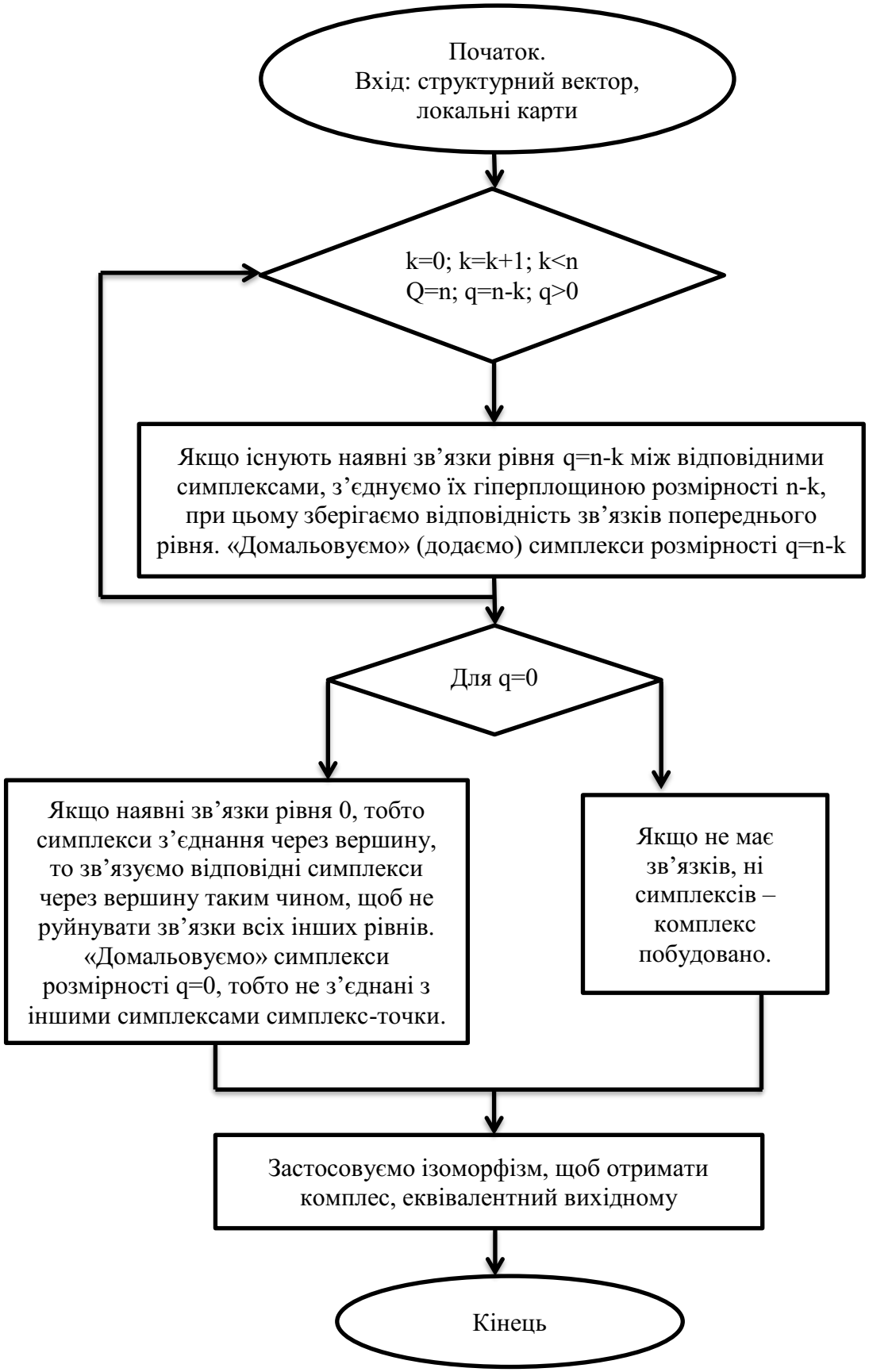


Рисунок 2.5 – Схема алгоритму відновлення симплеціального комплексу

Алгоритм відновлення симплеціального комплексу є наступним (рисунок 2.5):

1) На рівні максимальної розмірності q=n «малюємо» симплекси розмірності, виходячи з локальної карти на цьому рівні.

2) Для q=n-k>0:

– Якщо наявні зв’язки рівня q=n-k між відповідними симплексами, з’єднуємо їх гіперплощиною розмірності n-k, при цьому зберігаємо відповідність зв’язків попереднього рівня. «Домальовуємо» симплекси розмінності q=n-k.

– Якщо не виконується будь-яка з умов, то переходимо на рівень q=n-k+1.

3) Для q=0:

– Якщо наявні зв’язки рівня 0, тобто симплекси з’єднання через вершину, то зв’язуємо відповідні симплекси через вершину таким чином, щоб не руйнувати зв’язки всіх інших рівнів. «Домальовуємо» симплекси розмірності q=0, тобто не з’єднані з іншими симплексами симплекс-точки.

– Якщо немає ні зв’язків, ні симплексів – комплекс побудовано.

4) Застосовуємо ізоморфізм, щоб отримати комплекс еквівалентний вихідному.

5) Алгоритм завершено.

На першому кроці формується підмножина вершин, що утворюють симплекси максимальної розмірності.

На наступному кроці відбувається приклеювання симплексів за схемою заданою локальною картою. При цьому, ототожнюються підсимплекси (грані) різних симплексів – кожний такий підсимплекс відповідає реальній підсистемі, яка є спільною частиною підсистем більш високого рівня. Тобто вершини, що його утворюють, ідентифікуються з точністю до перестановки, але відповідно до інформації про з’єднання підсистем. При наступних склеюваннях можливе уточнення відповідності між вершинами комплексу (точками) та реальними елементарними (неструктурованими) підсистемами.

Деякі вершини однозначно співвідносяться з такими системами, а деякі з точністю до перестановки, що характеризується присутністю в системі складної симетрії [2].

Найбільша складність при постобробці алгоритму пов'язана із правильним визначенням ізоморфізму, який корегує неточності топології. Особливо важливо відслідковувати симплекси, які з'єднані через один і той самий симплекс меншої розмірності. Наприклад, три 2-симплекси з'єднані між собою через 0-симплекс. Але при перевірці за допомогою локальних карт відповідного рівня з'ясовується та зображується, яким чином і які саме симплекси поєднані. Ізоморфізм, у свою чергу, коригує симплекси, щоб побудований симплекс відповідав дійсності.

Система вразливостей в компанії може змінюватися з часом, адже різновиди вірусів та віртуозності кіберзловмисників вдосконалюються. Важливо вчасно вживати заходи для забезпечення протидій кібератакам. Основним завдаванням є підтримка обізнаності працівників. Але не менш важливо вчасно оновлювати програмне забезпечення та підтримувати цілісність інформаційних систем. Саме для цього може стати у нагоді інформація про структурованість всіх систем у компанії.

Запропоновані нами алгоритми дозволяють ідентифікувати приховані зв'язки, що потенційно можуть стати вразливими сторонами в системах, які використовують чутливу конфіденційну інформацію.

Для того, щоб оцінити ризики, які можуть бути породжені цими прихованими зв'язками і, як наслідок, збитками, компанії можуть використовувати моделі оцінювання ризиків, які ми розглядатимемо в наступному підрозділі.

2.2. Класифікація вразливостей за допомогою Q-аналізу

Вище було розглянуто алгоритми Q-аналізу для дослідження структури складних систем. Ця система алгоритмів являє собою метод для аналізу будь-якої системи, в якій зв'язки можуть бути не такими тривіальними, як бінарні в

графах. У цьому розділі представимо класифікацію вразливостей у залежності від їх ступеня зв’язності та впливу на потенційні загрози у системі.

Проведемо аналогії між симплеціальним комплексом та взаємозв’язком між уразливостями в системі. При аналізі вразливостей потрібно врахувати декілька факторів.

По-перше, виявити реальні та потенційні вразливості. Для цього, як було описано в розділі 1, необхідно провести інвентаризацію інформаційних ресурсів системи для виявлення потенційних та реальних уразливостей.

По-друге, описати наскільки критичною є кожна вразливість. Це може залежите від того, в якій підсистемі виникає дана вразливість, чи викликає вона каскадні вразливості, які загрози виникають при потенційному використанні даної вразливості, та наскільки є критичними загрози, викликані вразливостями.

Також однією з особливостей вразливостей є те, що уразливості одної підсистеми можуть впливати на вразливості та загрози іншої. Але така ситуація носить лише теоретичний характер, оскільки в реальних системам проявляється занадто рідко. Тому на практиці виявляємо взаємозалежності між уразливостями через потенційні загрози в рамках одної системи.

Як зазначено вище, існує циклічна залежність між такими послідовними подіями, як уразливості, загрози, атаки та інциденти. Наявність або виникнення кожної з цих подій не обов’язково призводить до виникнення наступної події, але ймовірність є високою. Тому наявність у системі, у тому числі й кіберсистемі, уразливості, створює потенційну загрозу, яка може призвести до атаки та інцидентів. Як було зазначено вище, управління та оцінка вразливостей позитивно впливає на інформаційну безпеку в цілому, та формує комплекс заходів (методику) щодо запобігання несанкціонованому вторгненню та мінімізації його негативних наслідків.

Класифікація та структурний аналіз системи вразливостей може суттєво допомогти у попереджені наслідків реалізації загроз.

Нижче наведено методологію структурного аналізу вразливостей.

Спочатку встановлюємо причинні зв’язки між загрозами та вразливостями. Будь-яка кіберсистема має певні вразливості. Найчастіше вони пов’язані з особливостями структури інформаційної системи, каналами зв’язку або ж з програмним забезпеченням та інструментами, які користувачі та розробники використовують у цій системі. У більшості випадків розробники мають уявлення, які вразливості притаманні їх продукту. Загальний опис та властивості уразливостей наведено в CVE [85]. Характерні особливості ІКС, аналіз якої здійснюється, статистичні дані про інциденти та загрози, які мали місце раніше, дозволяють зробити висновки про те, які вразливості викликають певні загрози. Використовуючи ці знання, можемо встановити причинні зв’язки між загрозами та вразливостями.

Наступний крок – побудова матриці інцидентності між загрозами та вразливостями. Побудова відповідної матриці надає загальне уявлення про взаємозв’язки між вразливостями. Але більш глибоке вивчення складної природи зв’язків між уразливостями та каскадними залежностями вимагає застосовування методології Q-аналізу.

Наведемо алгоритм проведення класифікації типів уразливостей у залежності від їх впливу на виникнення загроз ІКС.

1. Визначається набір уразливостей, притаманних ІКС, яка досліджується.

2. Визначаються загрози ІКС, які потенційно провокуються її відповідними уразливостями.

3. Будується матриця інцидентності для загроз і вразливостей ІКС.

4. Застосовується алгоритм побудови симплеціального комплексу ІКС.

5. Застосовується алгоритм побудови структурного дерева та локальних карт.

6. Використовується алгоритм локальних карт, для оцінки взаємозв’язків між уразливостями ІКС .

7. Використовується алгоритм пошуку нащадків для складно зв’язних уразливостей. Цей алгоритм допомагає виявити ієрархію вразливостей.

8. Проводиться класифікація загроз на основі характеристик відповідного симплексу в симплеціальному комплексі.

Останній пункт має вирішальне значення, оскільки дані, отримані за результатом здійснення Q-аналізу, дозволяють проводити класифікацію вразливостей за декількома характеристиками [3].

Класифікація за ступеню зв'язності, тобто визначення того, наскільки пов'язана або сумісна окрема вразливість з іншими. Якщо рівень q-зв'язності дорівнює 0, то вразливість існує незалежно від інших. Якщо, наприклад, q=3, то ця вразливість сама по собі не виникає, а тісно взаємопов'язана з наявністю двох інших уразливостями.

Класифікація за розмірністю примикання. Така класифікація базується на групуванні уразливостей, виходячи з максимального ступеня зв'язку між симплексами та пов'язана з власною розмірністю симплексів. Вона є свідченням того, наскільки сильно симплекси взаємопов'язані між собою, що, у свою чергу, відображає і ступінь їх впливу один на одного. Цю розмірність зв'язку можна виявити через зв'язки між симплексами на локальних картах.

Класифікація за кількістю нащадків. Ця характеристика відображає ступінь впливу певної вразливості на інші, тобто породження з однієї вразливості декількох інших. Така класифікація може бути корисною для оцінки критичності тої чи іншої вразливості. Очевидно, що наявність компоненту небезпеки, який породжує появу додаткової небезпеки має вищу оцінку впливу.

Наведемо підходи, на яких базується кожна класифікація. Класифікація за ступенем зв'язку показує, наскільки кожна вразливість сильно пов'язана з іншими вразливостями в горизонтальній площині. У матриці, яка була отримана під час побудови симлеціального комплексу, відображено ступінь взаємозалежності кожного симплексу вразливостей. Симплексом вразливостей може бути, як будь яка окрема вразливість, так і набір уразливостей, які виникають, по суті, одночасно. Зв'язки в симплексі також можуть бути не тривіальні, тобто n-арні. Число, яке відповідає за ступінь зв'язності в матриці

симлеціального комплексу, відображає силу зв'язності між симплексами, а, отже, і вразливостями. Із погляду інформаційної безпеки, такий підхід дає уявлення про наявність суміжних загроз, можливо, непрямої дії та із прихованими зв'язками.

Класифікація за розмірністю примикання визначається впливом не конкретної вразливості, а певного набору з них, зібраному в симплекси. Симплекси взаємозалежності вразливостей – це структура в комплексі системи вразливості.

В цьому дослідженні такий зв'язок відповідає одночасному виникненню вразливості. Це означає, що якщо в системі присутня хоча б одна з уразливостей симплексу, то вона може провокувати виникнення і інших уразливостей, не зважаючи на те, що вони можуть не викликати інші загрози. Розмірність зв'язку між симплексами вказує на те, наскільки сильний і якої арності є вплив окремого симплексу на інший та на увесь комплекс в цілому. Це важливо, оскільки такі залежності також дозволяють відслідковувати приховані зв'язки між уразливостями. Така стратегія допомагає попередити потенційні загрози і більш широко проаналізувати причини виникнення інцидентів у системі.

Класифікація за кількістю нащадків характеризує вертикаль зв'язків або каскади зв'язків. «Нащадки», які виникають унаслідок певних взаємозв'язків між одними вразливостями, характеризуються тим, що навіть при ліквідації більшості вразливостей в системі, деякі з них можуть залишатися. Наприклад, є симплекс зв'язків між уразливостями, при ліквідації деяких із них, або навіть усіх, залишаються такі вразливості, які продовжують опосередковано впливати на систему, тобто наслідки від таких уразливостей мають певний влив навіть при їх усуненні. Зазвичай ці вразливості є наслідком, або елементом технологій та інструментів, за допомогою яких побудована ІКС, аналіз якої здійснюється. Такі вразливості не можна усунути повністю, але обов'язково потрібно їх відпрацьовувати, формуючи комплекс превентивних/ заходів щодо можливих загроз та атак. Найчастіше такі вразливості мають

високе число q-зв'язку у матриці зв'язності, також їх можна назвати апріорними вразливостями, тобто позбутися від яких майже неможливо.

Приклад

Розглянемо застосування методів класифікації вразливостей на основі прикладу, запозиченого зі статті [57]. У таблиці 2.1 наведені пояснення зв'язків між загрозами та вразливостями.

Таблиця 2.1 – Зв'язок загроз і вразливостей у хмарних сховищах

№ з/п	Загроза	Опис загрози	Уразливості	Подія (інцидент)
1.	DB	Порушення даних (Data Breaches)	V1, V3, V4, V5, V7	Зловмисник може використовувати кілька методів атаки, зокрема SQL, впровадження команд і міжсайтовий сценарій. Уразливості – зловмисник отримує доступ до даних та можливість їх вилучення.
2.	IAM	Слабкі ідентифікація, управління обліковими даними та доступом до них (Weak Identity, Credential and Access Management)	V1, V3	Зловмисник може скористатися відсутністю багатофакторної автентифікації або використанням користувачем слабкого пароля.
3.	API	Недостатньо захищені інтерфейси програму-вання додатків (API) (Insecure interfaces APIs)	V1	Зловмисник може скористатися слабкістю у використанні інтерфейсів програмування додатків (API - Application Programming Interface), зокрема в протоколі обміну структурованими повідомленнями в розподілених обчислювальних системах SOAP (Simple Object Access Protocol), помилок у протоколі передачі гипертекста (HTTP – Hyper Text Transfer Protocol) тощо.
4.	SV	Системні	V4, V5, V6,	Зловмисник може атакувати через

		уразливості (Systesm Vulnerabilities)	V7	уразливості в образах віртуальних машин, гіпервізорах і віртуальних мережах.
5.	AH	Викрадення облікового запису (Account Hijacking)	V1	Для отримання доступу до системи зловмисник може використовувати обліковий запис жертви.
6.	MI	Зловмисні інсайдери (Malicious Insiders)	V5, V7	Зловмисник може створити образ віртуальної машини, що містить зловмисне програмне забезпечення, а потім поширити його.
7.	APT	Розширені стійкі загрози (Advanced Persistent Threats)	V1, V4, V5, V6, V7	Кормовий зловмисник може використовувати декілька типів уразливостей із певної віртуальної хмари або API для постійного зараження помилками цільової системи, головним чином для очищення даних
8.	DL	Втрата даних (Data loss)	V3, V4, V7	Зловмисник може використовувати методи атаки на основі дані, щоб отримати конфіденційну інформацію від інших віртуальних машин, які розташовані та тому ж самому сервері, або використати ризики резервного копіювання даних у процесі їх зберігання для очищення даних.
9.	IDD	Недостатня належна перевірка (Insufficient Due Diligence)	V4, V6	Зловмисник може використати недоліки у дотриманні правил у використанні хмарного середовища, зокрема конфігурації віртуальних машин, даних і спільних технологій.
10.	ANU	Зловживання та неналежне використан-ня хмарних сервісів (Abuse and Nefarious Use of Cloud Services)	V4	Зловмисник може атакувати за допомогою використання та спільного використання серверів, даних клієнтів за допомогою анонімного облікового запису.
11.	DOS	Відмова в обслуговуванні (Denial of Service)	V1, V2	Зловмисник може запросити додаткові IT-ресурси, тому авторизовані користувачі не зможуть отримати доступ до хмарного середовища.

12.	STV	Уразливості спільних технологій (Technology Vulnerabili-ties)	V4, V6	Зловмисник може перехопити та підробити віртуальні мережі або скористатися гнучкою конфігурацією гіпервізорів віртуальних машин для експлуатації.

Базуючись на даних таблиці 2.1, будуємо матрицю інцидентності зв'язку загроз і вразливостей у хмарних сховищах, наведену у таблиці 2.2.

Таблиця 2.2 – Матриця інцидентності зв'язку загроз і вразливостей в хмарних сховищах

Загрози/ вразливості	**V1**	**V2**	**V3**	**V4**	**V5**	**V6**	**V7**
DB	1		1	1	1		1
IAM	1		1				
API	1						
SV				1	1	1	1
AH	1						
MI					1		1
APT	1			1	1	1	1
DL			1	1			1
IDD				1		1	
ANU				1			
DOS	1	1					
STV				1		1	

Використовуючи алгоритм переходу від матриці інцидентності до матриці симплеціального комплексу, отримуємо матрицю, наведену у таблиці 2.3.

Таблиця 2.3 – Матриця симлеціального комплексу загроз

	DB	**IAM**	**API**	**SV**	**AH**	**MI**	**APT**	**DL**	**IDD**	**ANU**	**DOS**	**STV**
DB	5	2	1	3	1	2	4	3	1	1	1	1
IAM	2	2	1	0	1	0	1	1	0	0	1	0
API	1	1	1	0	1	0	1	0	0	0	1	0
SV	3	0	0	4	0	2	4	2	2	1	0	2
AH	1	1	1	0	1	0	1	0	0	0	1	0

MI	2	0	0	2	0	2	2	1	0	0	0	0
APT	4	1	1	4	1	2	5	2	2	1	1	2
DL	3	1	0	2	0	1	2	3	1	1	0	1
IDD	1	0	0	2	0	0	2	1	2	1	0	2
ANU	1	0	0	1	0	0	1	1	1	1	0	1
DOS	1	1	1	0	1	0	1	0	0	0	2	0
STV	1	0	0	2	0	0	2	1	2	1	0	2

Застосовуючи алгоритм побудови структурного дерева та структурного вектора, отримуємо структурне дерево для вразливостей хмарних сховищ, яке наведене на рисунку 2.6.

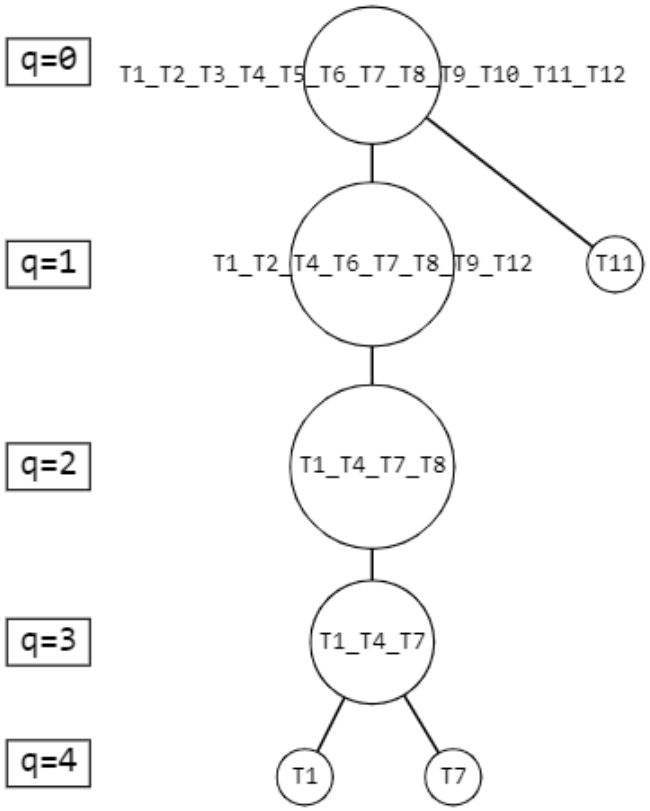


Рисунок 2.6 – Структурне дерево для вразливостей хмарних сховищ

При цьому, структурний вектор буде виглядати наступним чином: Q={2,2,3,2,2,1}.

Ураховуючи вищенаведене, відбудовуємо локальні карти для загроз хмарних сховищ, які наведені на рисунку 2.7, а також структурні графи (А-Д) зв’язку на рівні q=$\overline{0,4}$, які наведені на рисунку 2.8.

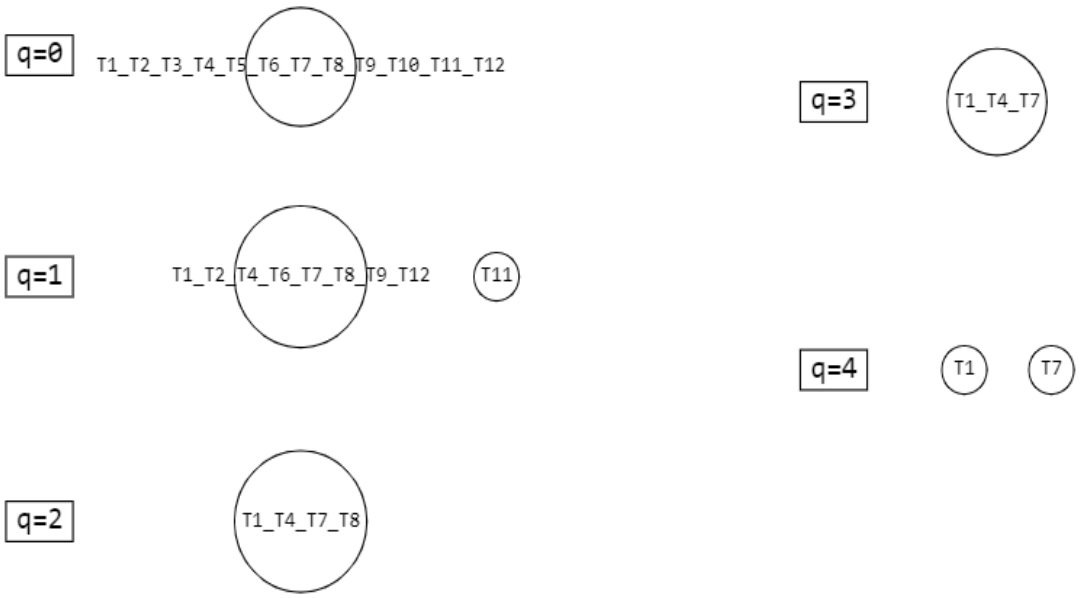
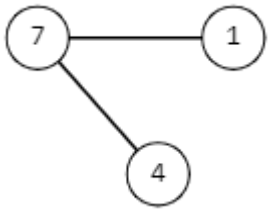
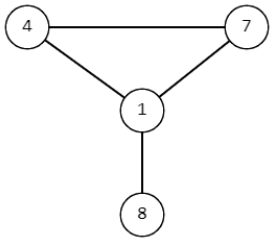


Рисунок 2.7 – Локальні карти для загроз хмарних сховищ

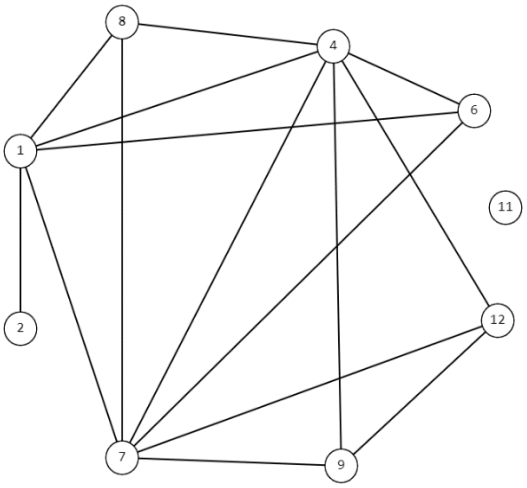
А)



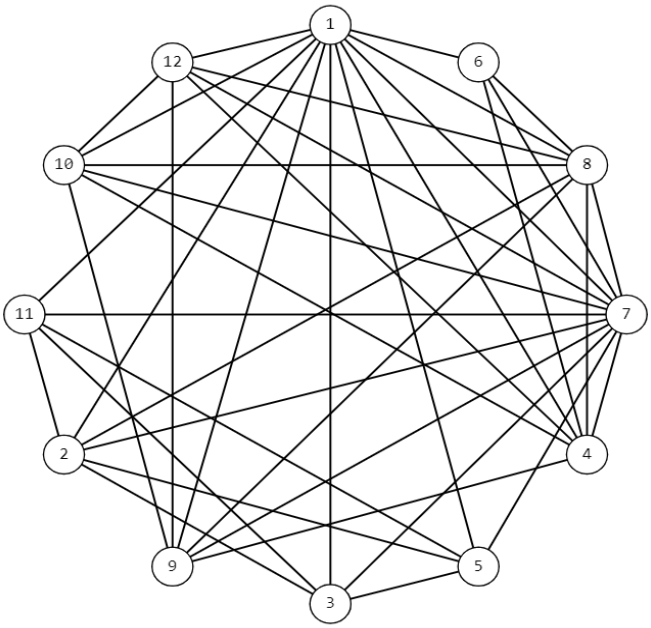
Б)



В)



Г)



Д)

Рисунок 2.8 – Структурні графи (А-Д) зв’язку на рівні q=$\overline{0,4}$

Проведемо аналіз нащадків з точки зору Q-аналізу.

Як зазначалося у попередній частині розділу, нащадок – це симплекс, породжений симплексом на попередньому рівні зв’язності. За цим принципом наведемо нащадків в цьому симлеціальному комплексі.

Загрози Т3, Т5, Т10 є структурними елементом в ланцюзі розмірності 0, тому не виокремлюються і не мають нащадків.

Загроза Т11 має лише одного нащадка тому, що виокремлюється на рівні q=1. Оскільки і розмірність самого симплекса, який відповідає цій загрозі теж дорівнює 1, то він не має великого рівня сумісності з іншими загрозами.

Загрози Т2, Т6, Т9, Т12 є структурними елементами в ланцюзі розмірності 1, тому не виокремлюються і не мають нащадків.

Загроза Т8 має схожі характеристики, але важливою її особливістю є те, що розмірність самого симплексу висока, а це означає, що симплекс є нащадком самого себе до рівня q=3.

Загроза Т4 має схожі характеристики, але важливою її особливістю є те, що розмірність самого симплексу висока, а це означає, що симплекс є нащадком самого себе до рівня q=4.

Загрози T1, T7 виокремлюються на рівні q=4. Вони породжують ланцюг симплексів, мають одного нащадка, що відповідає сильному взаємозв'язку розмірності q=3 та високої розмірності q=4.

Здійснивши структурний Q-аналіз, отримуємо вихідні дані для класифікації вразливостей.

За першою класифікацією маємо 6 рівнів еквівалентності:

q=0 – не має поділу на ланцюги;

q=1 – має поділ на 2 ланцюги;

q=2 – має поділ на 1 ланцюг;

q=3 – має поділ на 1 ланцюг;

q=4 – залишаються два симплекси з попередніх рівнів.

Відповідні ланцюги згруповані за рівнями зв'язності на подібні за впливом зв'язку від уразливостей.

Наступна класифікація відображає рівень впливу симплексів на інші симплекси, а також ступінь цього впливу. Для прикладу розглянемо локальні карти на кожному рівні:

q=0 – ураховуючи структурне дерево (рисунок 2.6), усі вразливості зв'язані в один ланцюг. Це вказує на можливу повну сумісність між загрозами через реалізацію вразливостей.

q=1 – симплекс T11 відокремлюється та має низьку сумісність з іншими загрозами. T3, T5, T10 є структурними елементами, не відокремлюється і мають низьку сумісність з іншими загрозами.

q=2 – T2, T6, T9, T12 є структурними елементами в ланцюзі, мають низьку сумісність з іншими загрозами.

q=3 – на цьому рівні T8 є структурним елементом в ланцюзі, має високий рівень сумісності з уразливостями, які відповідають тетраедру в топології симплеціального комплексу, при цьому зв'язки між різними загрозами не завжди бінарні.

q=4 – з ланцюга загроз виокремлюються T1, T7. На цьому рівні зв'язності вони виникають не сумісно, але кожна з них має великий вплив на

значну частину загроз. Вони мають більш високий ступінь q-зв'язності, оскільки мають вплив на значну кількість загроз. Т4 вилучається з ланцюга, що вказує на його сумісність з Т1, Т7, тобто вони є структурними частинами ланцюга і виникають сумісно з іншими загрозами.

Остання класифікація базується на кількості нащадків і відповідає за причино-наслідкові зв'язки між окремими вразливостями та ланцюгами у ланцюгах, а, отже, і породженими ними загрозами. Такий підхід може виявити, які вразливості мають більш загальний вплив, а які – більш локальний, коли наявність такої вразливості в системі не призводить до каскадного прояву інших.

Виходячи із наведеного вище аналізу, класифікація відповідних загроз виглядає наступним чином:

Т1, Т7 – загрози вищого рівня небезпеки, залежні від значної частини вразливостей системи.

Т4 – структурний елемент високого рівня зв'язку, на рівні 3.

Т8 – структурний елемент високого рівня зв'язку, залежить від значної частини вразливостей, але вже на рівні q=2 стає не сумісним з іншими загрозами, що характеризує її ізольованість.

Т2, Т6, Т9, Т12 – структурні елементи низького рівня зв'язку q=1, залежать від не значної частини вразливостей, але вже на рівні q=1 стають не сумісними з іншими, що характеризує ізольованість вразливостей, які на них впливають.

Т3, Т5, Т10 – структурні елементи низького рівня зв'язку q=0, які залежать від не значної частини вразливостей, але вже на рівні q=0 стають не сумісними з іншими вразливостями, що характеризує найбільшу ізольованість уразливостей, які на них впливають.

Т11 відокремлюється на рівні q=1. Оскільки і розмірність самого симплекса, який відповідає цій загрозі теж дорівнює 1, то вона не має великого рівня сумісності з іншими загрозами. Має одного нащадка.

Класифікація для нащадків відповідає загальній класифікації для наведених загроз. Особливість такого підходу полягає в тому, що його можна здійснювати, як на горизонтальному, вертикальному рівнях, або у вигляді ієрархічної структури. У залежності від цілей досліджень та визначених завдань для прийняття рішень, доцільно використовувати або окремо кожну з цих класифікації, або їх комбінацію. Це не вплине на остаточний результат, але дозволить розглянути проблему з різних точок зору.

2.3 Обернена задача Q-аналізу, структурний синтез системи

У першому підрозділі описано алгоритм оберненої задачі Q-аналізу. Зміст завдання полягає в тому, щоб відновити структуру системи, маючи лише структурне дерево та локальні карти. Але для відтворення симлеціального комплексу необхідно мати алгоритм переходу від матриці інцидентності до локальних карт та структурного дерева.

У ході дослідження проведено аналіз між уразливостями та загрозами. Наведений приклад використовувався в статті [57]. Пропонуємо основні викладки. Використовуємо звіт компанії Edgescan [79]. Нижче наведена статистика вразливостей, що виникають найчастіше (таблиця 2.4).

Таблиця 2.4 – Співвідношення вразливостей від загроз

Вразливість	**Назва**	**Загроза**	**Відсоток використання вразливості**
V1	Міжсайтовий сценарій (відображений) (Cross-Site Scripting (XSS) (reflected))	T1,T2, T3, T4	49.8%
V2	Порушена автентифікація, або погане керування сеансом, з можливим повним перебором (Broken Authentication/Poor Session Management, Brute Forcing Possible)	T3,T4	22.1%
IV3	Відслідковування шляху до файлу/Розкриття інформації/Розкриття вихідного коду (File path traversal/Information disclosure/Source Code Disclosure)	T1, T4	6.9%

V4	Проблема авторизації – підвищення привілеїв (Authorisation Issue – Privilege Escalation)	T3	6.0%
V5	Обхід шляху до файлу/прямий доступ до об’єктів File path traversal/Direct Object Access	T4	5.1%
V6	Завантаження зловмисного файлу (Malicious File Upload)	T5	3.2%
V7	Атаки десеріалізації (Deserialization Attacks)	T1	3.2%
V8	Впровадження виконуваного коду файлу Executable Code injection	T2, T3, T5	2.8%
V9	Впровадження зовнішньої сутності стандарту побудови мов розмітки ієрархічно структурованих даних для обміну між різними додатками– XML (Extensible Markup Language) XML External Entity Injection (XXE)	T3	2.3%
V10	Підробка запитів на стороні сервера Server-Side Request Forgery (SSRF)	T1, T5	1.8%

У цій таблиці також наведено поширений зв’язок між уразливостями та загрозами. Загальна характеристика залежності загроз від уразливостей виглядає так:

– Загроза працездатності сайту та збереження даних користувача призводить до фінансових і репутаційних втрат компанії (T1).

– Хакери використовують сайт для атак на інші ресурси, для розсилки спаму або проведення DoS атак. Сайт блокують пошуковики і браузери, і він втрачає користувачів (T2).

– Атака на сайт в корпоративному середовищі може бути точкою входу хакерів до корпоративної мережі компанії (T3).

– Атаки на системи електронної комерції можуть бути використані для здійснення шахрайських дій, викрадення клієнтських баз тощо (T4).

– Атаки можуть бути націлені на подальше «зараження» користувачів сайту, наприклад, за допомогою засобів експлуатації вразливостей браузерів чи їх компонентів (T5).

Ураховуючи дані, наведені у таблиці 2.4, будуємо матрицю інцидентності між уразливостями та загрозами (таблиця 2.5).

Таблиця 2.5 – Матриця інцидентності між уразливостями та загрозами

	V1	**V2**	**V3**	**V4**	**V5**	**V6**	**V7**	**V8**	**V9**	**V10**
T1	**1**		**1**				**1**			**1**
T2	**1**							**1**		
T3	**1**	**1**		**1**				**1**	**1**	
T4	**1**	**1**	**1**		**1**					
T5						**1**		**1**		**1**

У подальшій роботі застосуємо алгоритм, який доповнює обернену задачу, наведену в першому пункті цього розділу. Цей алгоритм надає можливість аналізувати систему, не будуючи при цьому сам симплеціальний комплекс. Основна мета дослідження полягає в тому, щоб визначити вплив уразливостей на функціонування системи, тому вважаємо, що сиплекси формуються по стовпцях.

1. Для побудови структурного дерева:

а. Ранжуємо стовпці по кількості одиниць. Найбільша кількість одиниць визначає глибину структурного дерева.

Таблиця 2.6 – Проранжована кількість залежностей вразливостей від загроз

V1	**V8**	**V3**	**V2**	**V10**	**V9**	**V7**	**V6**	**V5**	**V4**
4	3	2	2	2	1	1	1	1	1

б. Рухаючись від симплекса з найбільшою розмірністю, формуємо кількість листів на кожному з рівнів:

– на кожному рівні зв’язності q=k домальовуємо листки дерева, розмірність яких дорівнює k;

– усі інші симплекси з q>k зливаються в одну вершину на цьому рівні;

– далі переходимо на рівень q=k-1.

Алгоритм завершується при q=0. На цьому рівні всі листки минулого рівня стають коренем дерева.

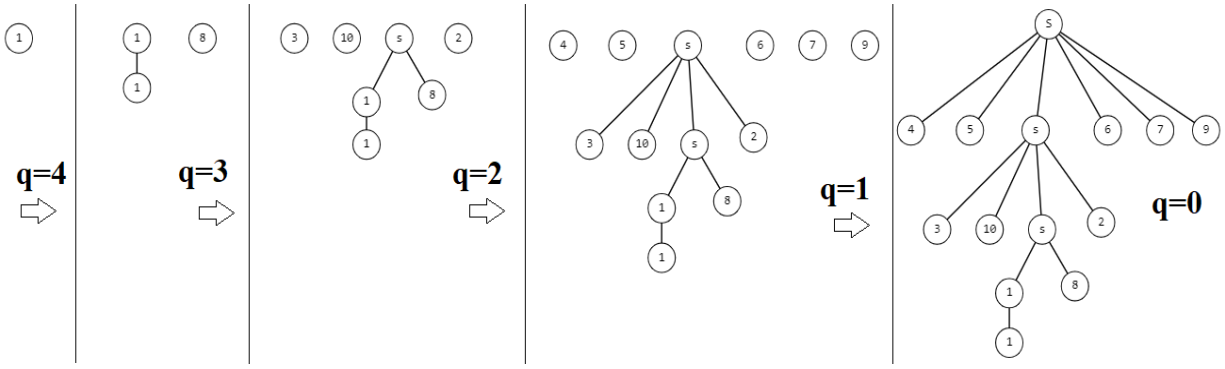


Рисунок 2.9 - Побудова структурного дерева на основі матриці інцидентності

Зробимо роз’яснення для рисунка 2.9 щодо побудови структурного дерева. На найнижчому рівні q-зв’язності знаходиться лише один симплекс, який відповідає вразливості V1. Таблиця інцидентності ілюструє те, як пов’язані симплекси.

На наступному рівні q=3 залишається V1 і від нього виходить ребро, таким чином відображається перехід з нижнього до верхнього рівня. З’являється V8, який не зв’язаний з V1, тому він просто домальовується.

На рівні q=2 V1 і V8 зливаються у ланцюг і стають «одним цілим», з точки зору, симплеціального комплексу. Виходячи з того, що рівень зв’язності тут 2, вони поєднуються між собою гранню. З попереднього рівня на поточний малюємо ребра від двох симплексів в один. На цьому рівні додаються вразливості V2, V3, V10. Вони не поєднані з іншими, тому домальовуються як окремі симплекси.

На рівні q=1 всі симплекси з попереднього рівня зливаються в один. З'єднані вони між собою по ребрах. Домальовуються симплекси, що відповідають V4, V5, V6, V7, V9.

На останньому рівні q=0 всі симплекси зливаються в комплекс.

2. Для побудови локальних карт:

а. На найвищому рівні q-зв'язності малюємо всі симплекси цієї розмірності.

б. На кожному рівні q=k:

– Всі симплекси (стовпці матриці) малюються як на рівні q=k+1. Для кожної пари симплексів проглядаємо строки матриці інцидентності. Якщо у рядку стоять одиниці для кожного з симплексів, то додаємо до лічильника q-зв'язку одиницю: $L = L + 1$ ($L \in \{0,1, \dots, q\}$).

– Якщо L=q малюємо ребро між парами симплексів.

– Якщо L<q – не малюємо ребро.

– Якщо L>q – ребро було домальовано на попередньому кроці.

– Домальовуємо симплекси розмірності q.

в. На рівні зв'язності q=0 мають бути домальовані всі симплекси розмірності 0. Усі ребра переносяться з попередніх рівнів та домальовуються ті, що зв'язані з цим рівнем.

3. Алгоритм завершено.

Виходячи з наведеного прикладу, розрахована таблиця 2.7 з попарними залежностями між уразливостями та загрозами.

По діагоналі таблиці розташовані суми кількості одиниць по стовбцю вразливостей.

Недіагональні елементи вираховуються наступним чином. Вибирається дві пари вразливостей, наприклад V1 та V8. Суми одиниць, для кожної з них, відповідно 4 і 3. Ураховуючи загрози, пов'язані з ними, бачимо, що дві з них одночасно відносяться і до V1, і до V8. Тому в матриці у клітинці, розташованій на перетині V1 та V8 пишемо 2. За таким принципом рахуємо всі інші елементи. Так як відношення між елементами еквівалентні з обох

сторін, то нам потрібно порахувати лише елементи верхнього трикутника цієї матриці, бо нижній буде симетричний верхньому.

Таблиця 2.7 – попередньо пораховані попарні збіг симплексів по строкам.

	V1	**V2**	**V3**	**V4**	**V5**	**V6**	**V7**	**V8**	**V9**	**V10**
V1	4	2	2	1	1	0	1	2	1	1
V2		2	1	1	1	0	0	1	1	0
V3			2	0	1	0	1	0	0	1
V4				1	0	0	0	1	1	0
V5					1	0	0	0	0	0
V6						1	0	1	0	1
V7							1	0	0	1
V8								3	1	1
V9									1	0
V10										2

Нижче наведена схема побудови локальних карт для кожного рівня q-зв’язності (рисунок 2.10). Використовуючи побудоване структурне дерево (рисунок 2.6 та таблиця 2.10), розглянемо, як функціонує алгоритм.

На найвищому рівні q-зв’язності розташовано V1, який – має найбільшу розмірність. Це виходить із матриці, бо немає більше елементів з цифрами 4 із дерева, оскільки на найнижчому рівні лише один симплекс.

Наступний рівень 3. На ньому з’являється V8. Але на перетині V1 та V8 зв’язок рівня 2, тому ребро між ними не можливо провести. Локальна карта складається з двох не поєднаних симплексів.

На наступному ріні зв’язності з’являються V2, V3, V10. V2, V3, V3 – зв’язані з V1 зв’язком порядку 2 (див. таблиця 2.7), тому малюємо між ними ребра, V10 – не зв’язаний з іншими нижчим зв’язком, тому зображений окремо.

На рівні q=1 з’являються симплекси розмірності 1: V4, V5, V6, V7, V9. Всі симплекси в більшості пов’язані між собою зв’язком розмірності 1, тому на цьому рівні всі симплекси певним чином пов’язані між собою.

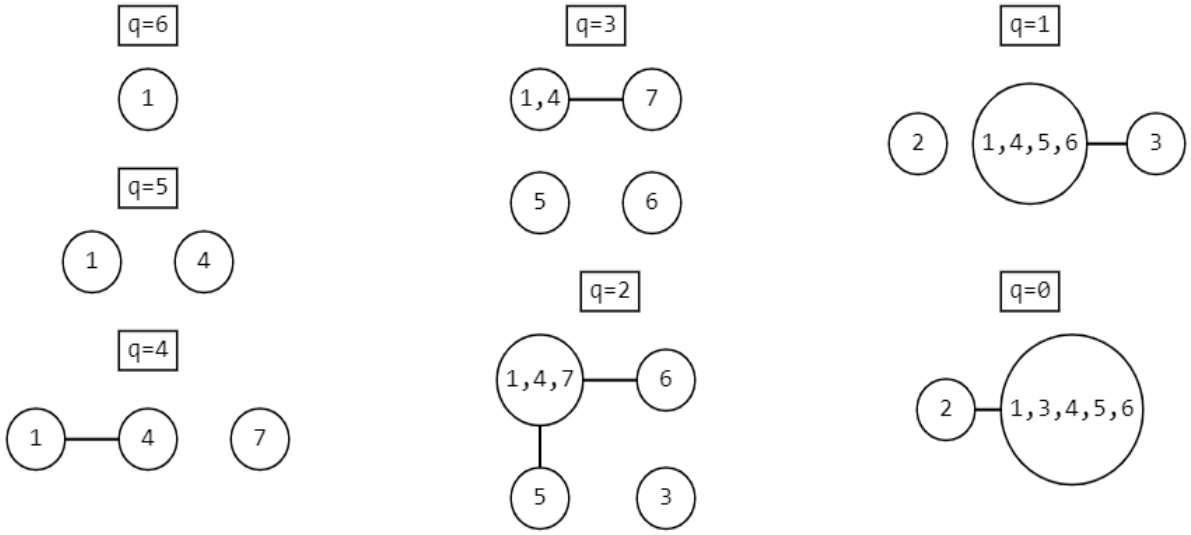


Рисунок 2.10 – Локальні карти для системи вразливостей

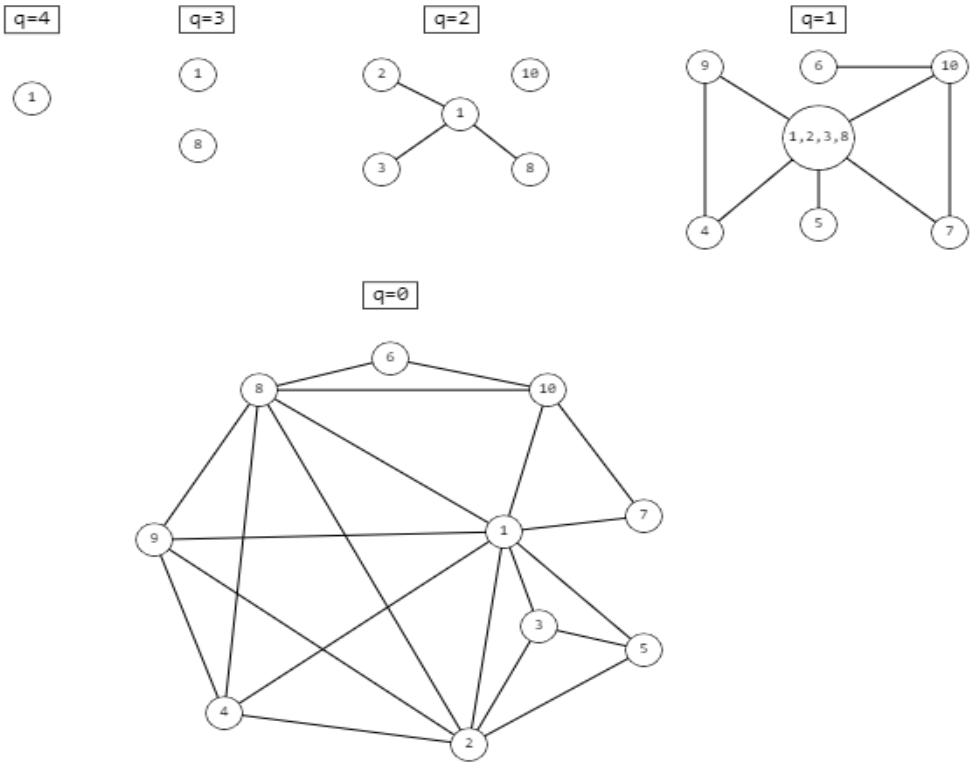


Рисунок 2.11 – Структурні графи на кожному рівні q-зв’язку.

Доповнений алгоритм оберненої задачі надає можливість проводити Q-аналіз, використовуючи лише матрицю інцидентності між структурними елементами.

Наведений вище приклад показує яким чином можливо проводити аналіз «прихованих» зв’язків між уразливостями, а також впливів тих, чи

інших уразливостей. Топологічний аналіз дозоляє розв’язувати ще й іншу задачу.

У разі, коли симплекси вважати загрозами, то можна побудувати симплеціальний комплекс загроз через уразливості та, відповідно, знайти додаткові взаємозв’язки між уразливостями та оцінити ступінь їх впливу на систему.

2.4 Зв’язки між задачами Q-аналізу

Класична задача Q-аналізу включає аналіз структури системи на основі побудованого для нього симплеціального комплексу. Але такий підхід є достатньо трудомістким у застосуванні, особливо в кібербезпеці.

Найчастіше представлення кіберсистем являє собою граф і відповідну до нього матрицю інцидентності. Тому в ході дисертаційного дослідження було розроблено методологію переходу від матриці інцидентності до симплеціального комплексу, а відтак – до структурного дерева та локальних карт.

У випадку, коли немає необхідності будувати симплеціальний комплекс, представлено алгоритм переходу від матриці до дерева та карт. Також розроблено алгоритм відновлення симплеціального комплексу з карт та структурного дерева. Наведений вище метод дає можливість з легкістю переходити від понять топології до графів, а також полегшує розуміння ІКС та здійснювати всебічний аналіз їх структури.

Для кращого розуміння нижче наведено схему взаємозв’язку між моделями на рисунку 2.12.

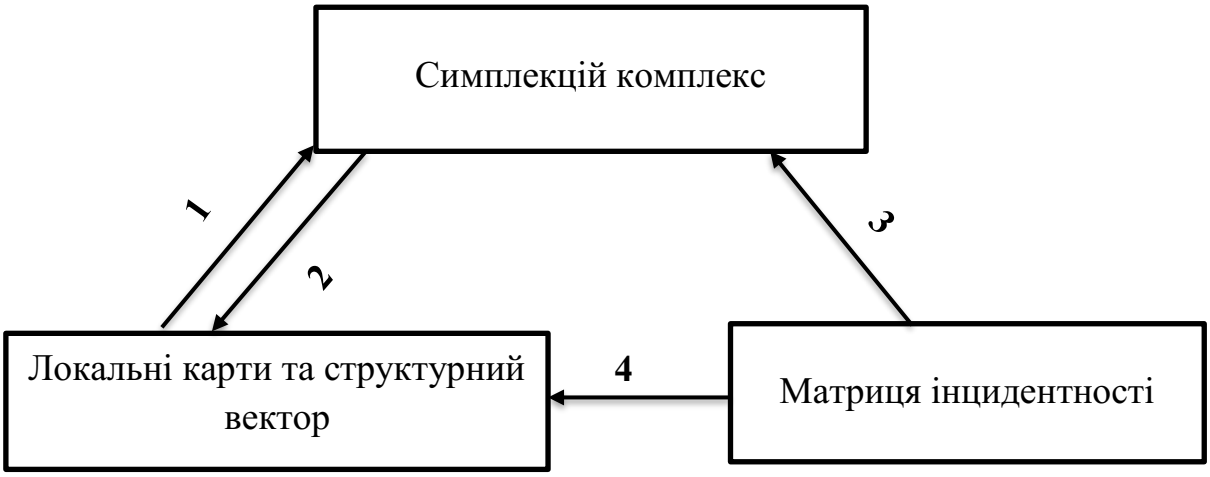


Рисунок 2.12 - Схематичний взаємозв’язок між методологіями Q-аналізу

Класичний Q-аналіз передбачає, що система, яку ми аналізуємо представлена у вигляді симлеціального комплексу, над яким виконуються деякі маніпуляції. Класичний Q-аналіз також передбачає, що досліджувана система представлена у вигляді симплеціального комплексу, для якого потрібно знайти структурні характеристики. Цей перехід показаний на рисунок 2.12 як дуга під номером 1. Тобто шукаються зв’язки, будуються локальні карти, обраховуються структурний вектор та структурне дерево.

У ході проведеного дослідження розроблено алгоритми та методи переходу від локальних карт та структурного дерева до симплеціального комплексу задля того, щоб була можливість відтворити геометричну модель системи за наявною інформацією про її структуру. Це відображено на схемі дугою 2.

Але найбільш корисною для практичного застосування виявляється розробка алгоритмів для переходу від матриці інцидентності до симплеціального комплексу (дуга 3), а також до локальних карт і структурного дерева, що відображено дугою 4.

Ця методологія є важливою, адже більшість взаємозв’язків між структурними одиницями в сучасних роботах описуються саме за допомогою матриць інцидентності.

У класичних дослідженнях опис переходу від матриці інцидентності до симплеціального комплексу наведено лише для окремих прикладів конкретних матриць.

Розроблені алгоритми дозволяють більш легко та широко застосовувати Q-аналіз для комп'ютерного пошуку складних та прихованих зв'язків у системі.

Висновки до розділу 2

У другому розділі наведені процедури визначення (знаходження) структурних характеристик інформаційної системи, які в подальшому використовуються для розрахунку оцінки ризику. Адже кожна виявлена структурна характеристика ІКС наочно відображає складні зв'язки між елементами системи вразливостей і відображає ступінь сумісності.

Розроблено алгоритми для переходу від матриці інцидентності до симплеціального комплексу, побудови структурного дерева, локальних карт, пошуку нащадків за ланцюгами симплексів. Зазначені вище алгоритми дозволяють достовірно та всебічно описати структуру системи вразливостей ІКС. Розроблена система показників описує взаємозалежності між загрозами та вразливостями, а також дозволяє визначити потенційні сумісні реалізації вразливостей.

Розроблені алгоритми для розв'язання оберненої задачі Q-аналізу дозволяють розширити сферу застосування моделей Q-аналізу для будь-якої структури системи вразливостей ІКС.

У цьому розділі описана класифікація вразливостей на основі примикання, q-зв'язків та кількості нащадків при наслідуванні. Ці показники структури для вразливостей відображають їх сумісність та можливості впливу на безпеку системи.

Доведено, що методи Q-аналізу дозволяють дослідити структуру складної системи та визначити зв'язки високих порядків, які складно відобразити та побачити безпосередньо за допомогою теорії графів. На основі

результатів Q-аналізу керівництво організації отримує можливість постановки задач щодо планування ресурсного забезпечення інформаційних підсистем, посилення або послаблення тих чи інших зв’язків у складній системі ІКС для забезпечення її захисту та покращення функціонування.

Ураховуючи наведене вище, розроблено та представлено методику, яка дозволяє аналізувати не лише загальну структуру самої системи, а й характер зв’язків між її підсистемами.

До переваг зазначеної методики слід віднести масштабованість, тобто можливість використання для систем будь-якого масштабу, зокрема тих, які мають велику кількість підсистем, а також можливість виявляти багатокомпонентні взаємовідносини між підсистемами неочевидні з першого погляду. Застосування відповідних алгоритмів також дозволяє автоматизувати процес визначення ланцюгів симплексів, структурного вектора, побудову структурного дерева, локальних карт та структурного графу системи.

Запропонований за результатами проведеного дослідження алгоритм синтезу симплеціального комплексу дозволяє побудувати модель топологічної структури системи для відображення багаторівневих зв’язків уразливостей та загроз.

Наведено практичне застосування запропонованих моделей та методів на прикладі залежності загроз та вразливостей у хмарному середовищі та мережевих структурах.

РОЗДІЛ 3

МЕТОД ОЦІНЮВАННЯ КІБЕРРИЗИКІВ НА ОСНОВІ СТРУКТУРИ СИСТЕМИ

3.1 Класифікація моделей ризиків у складних кіберсистемах

В дисертаційній роботі розглядаються не очевидні залежності між уразливостями та загрозами. Такі взаємозв'язки породжують каскадні залежності або зв'язки більш високого рангу, ніж у звичайних графах. У попередньому розділі було представлено структурний аналіз та класифікацію за допомогою Q-аналізу. Також наведена методологія переходу від графу до сиплекційного комплексу для кращого представлення зв'язків між уразливостями та загрозами. Досліджено, що традиційного підходу та методу обрахунку ризиків недостатньо для опису ризиків для систем зі складною структурою. Тому вони вимагають удосконалення для більш всебічного та якісного відображення структурних особливостей інформаційної системи.

У першому розділі представлено аналіз існуючих підходів для розрахунку ризиків та пошуку вхідних даних для нього. У випадку кіберінцидентів при оцінці ризиків, складність виникає як при оцінці ймовірностей, так і масштабів збитків. Також виникають проблеми, пов'язані з тим, що в кіберпросторі важко оцінити всі втрати, адже найбільше страждає репутація організації. Намагання відновити довіру може не досягнути бажаних результатів та призвести до ліквідації організації.

За результатами проведеного дослідження запропоновано метод обрахунків ризиків, який дозволяє врахувати складні зв'язки елементів системи, а також уразливості, які виникають у процесі її життєвого циклу.

Розглянемо деякі приклади.

Використовуємо класичну байєсову формулу (3.1) для розрахунку ризиків:

$$R = \sum_i \ p_i V_i, \tag{3.1}$$

де p_i – ймовірність настання події (реалізація вразливості), V_i – розмір втрат у разі реалізації події, $i = \overline{1,n}$ – індекс вразливості.

Ця формула зазвичай дуже абстрактна і не враховує особливості зібраних вхідних даних. Основним недоліком цього підходу, як було зазначено раніше, є ситуації, коли загальна сума втрат від інцендентів унаслідок реалізації уразливостей та загроз, що трапляються доволі часто та окремо не призводять до значних збитків, можуть за загальним обсягом втрат дорівнювати інцидентам з низькою ймовірністю, але з великими втратами.

Для врахування особливостей взаємозв'язку між уразливостями пропонується застосовувати модель взаємодії та впливу між уразливостями на основі Q-аналізу з урахуванням структурних особливостей, що виникають при побудові симлеціального комплексу. Загальну схему формування байєсової оцінки ризиків на основі втрат та ймовірностей наведено на рисунку 3.1.

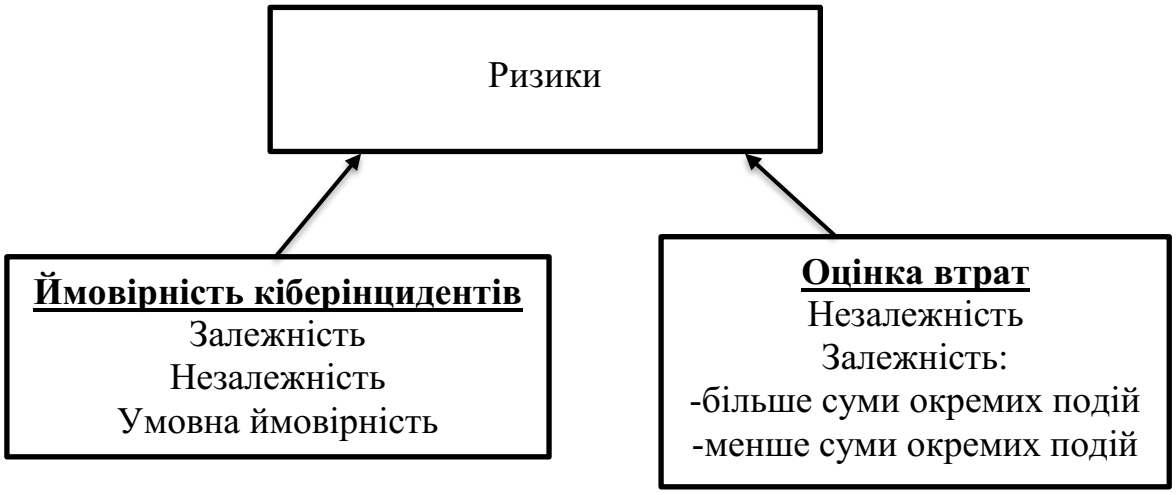


Рисунок 3.1 - Схема уточнень оцінки ризиків

У ході дослідження проводились уточнення оцінок відповідних ймовірностей та втрат. Класична формула середніх втрат ураховує сумісність та залежність несприятливих подій, але, зазвичай, оцінка ймовірностей реалізації загроз спрощується для ситуації окремих несумісних подій.

У реальності можуть траплятися сумісні реалізації вразливостей/загроз, що ускладнює оцінки ймовірності внаслідок виникнення сумісних та умовних

ймовірностей. Уточнення оцінки ризику відбувається також за рахунок модифікації оцінки величини збитків у разі виникнення таких подіях.

Зрозуміло, що у разі, коли відповідні вразливості незалежні, то сумарні збитки від їх сумісної реалізації дорівнюють сумі збитків від окремих інцидентів. При цьому, рівень втрат розглядається як функція, що залежить від втрат унаслідок кожної події, ураховуючи випадок сумісної реалізації залежних уразливостей. При цьому, втрати можуть збільшуватися чи зменшуватися у порівнянні з лінійною оцінкою. Наприклад, у тому випадку, коли події не мають значного впливу на систему, тоді більш ефективним способом подолання негативних наслідків є одночасна обробка декілька подій.

Але можуть траплятися випадки, коли сумарний збиток від подій більший за суму збитків від окремих випадків. Наприклад, якщо реалізований ризик привів до краху системи. Це випадок, коли окремі поодинокі події завдають системі відповідної шкоди, але система залишається життєздатною, а через одночасну реалізацію тих самих подій система може втратити свою життєздатність.

Нижче наведено класифікацію потенційних випадків побудови такої оцінки для ризику та втрат.

У разі, коли вразливості подій несумісні, застосовуються класичні підходи до оцінки ризику.

1.0. Формула (3.2) розрахунку ризику у випадку, коли вразливості при реалізації подій несумісні:

$$R = \sum_i p_i V_i, \tag{3.2}$$

де $\sum_i p_i < 1$ та $\exists p_0 > 0$ – ймовірність функціонування ситеми без втрат, V_i – втрати від подій.

Ця формула ідентична тій, що наводиться в класичній оцінці ризику. Єдине уточнення – сума ймовірностей менша за одиницю, бо можуть бути доданки, у яких велична збитків буде дорівнювати нулю. Це означає, що,

навіть, у разі, коли існує ймовірність виникнення деяких збитків, їх сумарна величина не значна у порівнянні з іншими можливими загальними втратами.

Наступні вразливості являють собою комбінації існування різного виду залежності між подіями.

2.0. Формула (3.3) розрахунку ризику у випадку парної сумісності вразливостей при реалізації подій і їх незалежності (ймовірнісна та за втратами):

$$R = \sum_{i} p_i V_i + \sum_{i,j,i \neq j} p_i p_j (V_i + V_j) \tag{3.3}$$

Ця формула описує випадок, коли окрім незалежного виникнення подій (збитків), існує попарна сумісна реалізація парних подій. Тобто є ймовірність виникнення попарно деяких або всіх подій одночасно. При цьому, оскільки окремі події є незалежними між собою, то сумісна вірогідність розраховується як добуток, а функція втрат розраховується як сума.

2.1. Формула (3.4) розрахунку ризику у випадку парної сумісності вразливостей при реалізації подій, їх ймовірнісної залежності та їх незалежності за втратами:

$$R = \sum_{i} p_i V_i + \sum_{i,j,i \neq j} p_{\{i,j\}} (V_i + V_j) \tag{3.4}$$

Ця формула відображає так само парну сумність. Тобто, можливість реалізації деяких подій одночасно, тому в другому доданку функція втрат відображає, як формуються загальні збитки (сума окремих збитків), але, при цьому, ураховується їх ймовірнісна залежність. Тобто, окремі події є взаємопов’язаними і виникають внаслідок інших подій. Наприклад, настання окремої події відбувається внаслідок іншої події або при одночасному виникненню декількох з них. Ймовірність при цьому не дорівнює добутку окремих компонентів, а розраховується за допомогою умовних ймовірностей, або визначається експертним шляхом.

2.2. Формула (3.5) розрахунку ризику у випадку парної сумісності і незалежності вразливостей при реалізації подій за ймовірністю та їх залежністю за втратами:

$$R = \sum_i p_i V_i + \sum_{i,j,i \neq j} p_i p_j V_{\{i,j\}}, \quad V_{\{i,j\}} \neq V_i + V_j \tag{3.5}$$

2.3. Формула (3.6) розрахунку ризику у випадку парної сумісності вразливостей при реалізації подій, їх ймовірнісної залежності та їх залежності за втратами:

$$R = \sum_i p_i V_i + \sum_{i,j,i \neq j} p_{\{i,j\}} V_{\{i,j\}}, \qquad V_{\{i,j\}} \neq V_i + V_j \tag{3.6}$$

Наступним випадком є випадок, коли існує не лише парна ймовірнісна залежність подій, але і залежність за втратами. Тобто при реалізації одночасно двох подій загальні збитки не дорівнюють сумі збитків від окремих випадків.

У разі, коли при настанні нескладних випадків реалізації ризиків, загальна сума збитків менша за суму збитків від окремих випадків, застосовується функція втрат. При цьому, у разі, коли відповідні ризики є критичними для системи, то загальні збитки можуть перевищувати суму збитків від окремих подій. Окрім цього, при врахуванні залежності подій від їх ймовірності, оцінка ризику стає більш трудомісткою, але більше враховує специфічні властивості і структуру системи.

Далі наводяться формули, які описують більш удосконалені підходи до оцінки ризиків, що враховують потрійну і більше сумісну залежність ризику від ймовірності та втрат. Викладки цих формул аналогічні наведеним вище формулам попарній сумісності подій, тому опис їх буде пропущено.

Більш інтерес представляють формули, які відображають розрахунок ризику у випадку повної сумісності подій та залежності їх від втрат та з урахуванням ймовірності їх виникнення.

n.0. Формула (3.7) розрахунку ризику у випадку повної сумісності вразливостей при реалізації подій та їх повній незалежності від ймовірності та втрат:

$$R = \sum_i p_i V_i + \sum_{i,j,i\neq j} p_i p_j (V_i + V_j) + \cdots + \prod_{i=1}^{n} p_i \sum_{i=1}^{n} V_i \quad (3.7)$$

n.1. Формула (3.8) розрахунку ризику у випадку повної сумісності, незалежності вразливостей при реалізації подій за ймовірністю і їх залежністю від втрат:

$$R = \sum_i p_i V_i + \sum_{i,j,i\neq j} p_i p_j V_{\{i,j\}} + \cdots + \prod_{i=1}^{n} p_i V_{\{i,j,\ldots,z\}} \quad (3.8)$$

n.2. Формула (3.9) розрахунку ризику у випадку повної сумісності вразливостей при реалізації подій, їх незалежності за втратами і залежністю від ймовірності:

$$R = \sum_i p_i V_i + \sum_i p_{\{i,j\}} (V_i + V_j) + \cdots + p_{\{i,j,\ldots,z\}} \sum_{i=1}^{n} V_i \quad (3.9)$$

n.3. Найбільш загальна формула (3.10) обчислення ризику, коли наявні всі можливі комбінації вразливостей при реалізації подій:

$$R = \sum_i p_i V_i + \sum_{i,j,i\neq j} p_{\{i,j\}} V_{\{i,j\}} + \sum_{i,j,k,i\neq j\neq k} p_{\{i,j,k\}} V_{\{i,j,k\}} + \cdots + p_{\{i,\ldots,n\}} V_{\{i,\ldots,n\}} \quad (3.10)$$

Для кожного листка структурного дерева загроз справедливі різні варіанти цієї формули для обрахунку ризику, а, отже, і для кожного симплексу сума ймовірності буде менша одиниці. Але в ході ускладнення на кожному рівні зв’язності при проходженні по структурному дереву збільшується і кількість доданків в формулі ризику. Для того, щоб однозначно вибудувати систему ризику потрібна побудова структурного дерева на основі Q-аналізу, алгоритм побудови якого висвітлений у розділі 2.

Остання серед наведених формул для розрахунку ризиків описує найскладніший варіант, коли опрацьовуються події з високим рівнем імовірності залежні одна від іншої. Тобто будь-яка з подій може запускати каскадом реалізацію різних комбінації інших подій. При цьому, оскільки ці події є сумісними, це означає, що така реалізація допускається.

Зазначена формула охоплює і випадки незалежної реалізації події з урахуванням збитків, і варіанти, коли загальна сума збитків є вищою або нижчою за суму збитків від окремих подій. Вона охоплює різні варіанти можливої реалізації подій. Розрахунок за цією формулою є достатньо трудомістким. При цьому, на практиці може статися, що ймовірності деяких подій достатньо не значні, або навіть нульові, або самі збитки не суттєві або нульові, тому їх можна не враховувати. Виходячи з цього, в мультиплікативній формулі відповідні доданки будуть дорівнювати нулю і ними можна знехтувати.

Запропоновану формулу, як правило, використовують для одного симплексу в комплексі. Доданки з більш складною структурою мають не такий значний вклад, адже їх ймовірності достатньо малі, а їх добутки – ще менші. Не зважаючи на те, що величина збитків, при цьому, зростає, це відбувається адитивно.

Зважаючи на вищенаведене, низькі ймовірності значно знижують вплив подій на можливий розвиток ситуації, незважаючи на те, що внаслідок цих подій організація може понести значні збитки. Тобто сумісність подій реалізується через наявність зв’язку між ними в симплексі.

3.2 Використання структурного аналізу для оцінок ризиків

Структурні особливості, які обумовлені симплеціальним комплексом, дозволяють в оцінках ризиків урахувати сумісність між уразливостями. Сумісність в цьому контексті означає, що в залежності від різних обставин одні і ті ж самі вразливості можуть виникати (реалізовуватися) одночасно або окремо. Виходячи з цього, при розрахунку ризиків такі ситуації слід враховувати, адже чим складніший зв’язок між окремими вразливостями, тим більшим є вклад окремих компонентів у загальний ризик.

Але специфіка цієї ситуації полягає в тому, що при обрахунку загального ризику ІКС від загальної суми ризиків потрібно віднімати ризики, які є зв’язками між ланцюгами симплексів. Оскільки вони враховуються як

при обрахунку ризиків окремих підсистем, так і при обрахунку повного ризику (приклад повної ймовірності). Тобто вплив таких зв'язків ураховується декілька разів. Коли розглядається комплекс в цілому, то відбувається дублювання зв'язків між уразливостями, які відносяться до різних симплексів, але через які відбувається «склеювання» симплексів. Тому про обрахунку загальної суми ризиків системи необхідно усувати ці повтори.

Розрахунок загального ризику починається з формули (3.11), яка враховує всі листя структурного дерева, а це симплекси різної розмірності:

$$R = \sum_{i} r_i + \cdots + \sum_{\{i,\dots,k\}} r_{\{i,\dots,k\}}, \tag{3.11}$$

де $i, \dots, k = \overline{1, N}$, і N - кількість симплексів.

Кожному листу структурного дерева (а це окремий ланцюг-симплекс) відповідає окрема частина загальної формули для обрахунку ризику. Але в процесі проходження по структурному дереву ускладнення ланцюгів на кожному рівні зв'язності і, відповідно, кількість доданків у формулі ризику збільшується. Таким чином, для того, щоб однозначно розрахувати оцінку повного ризику, необхідно застосувати процедуру синтезу симплеціального комплексу, запропоновану у другому розділі роботи.

Доведено, що запропоновані структурні особливості симплеціального комплексу дозволяють ураховувати при оцінюванні ризику сумісність між загрозами та вразливостями. Сумісність в цьому контексті означає, що окремі вразливості, у залежності від різних обставин, можуть ініціюватись (реалізовуватися) або одночасно, або окремо. При цьому, встановлено, що чим складніший зв'язок між окремими вразливостями, тим більший вклад сумісних компонентів у загальний ризик.

При обрахунку загального ризику системи також необхідно враховувати «місця склеювання» (примикання) між ланцюгами симплексів. Оскільки ці місця є симплексами за визначенням, ризик, що відповідає цьому ланцюгу, формується з двох ланцюгів за місцем примикання. Обчислюється сума

ризиків для двох ланцюгів, від якої віддимається ризик для симплекса примикання, оскільки відбувається його дублювання для кожного окремого ланцюга.

У разі, коли розглядається «к» ланцюгів, то примикання по симплексу відбувається для всіх ланцюгів разом. Зрозуміло, що для компенсації кратності примикання від суми ризиків по ланцюгах необхідно віднімати ризик по симплексу множений на (*к-1*).

Виходячи з цього, загальну суму ризиків (по ланцюгах) необхідно корегувати з урахуванням таких повторів для кожної вершині структурного дерева.

Інформація щодо структури примикання міститься у локальній карті та структурному графі комплексу, і може бути використана для розрахунку ризику за допомогою них безпосередньо.

В цілому розрахунок ризику нагадує відомі алгоритми «згортання дерева» з теорії рішень, але із урахуванням «включень та виключень» і відповідної кратності примикання.

Отже, описана вище загальна оцінка ризиків для комплексу системи в цілому розраховується за формулою (3.12):

$$R_{\text{загал.}} = R - R^* \tag{3.12}$$

У наведеній формулі R – це той ризик у системі, що визначається симплексами – компонентами комплексу, з яких він «склеюється». Але він надмірний, бо містить повтори, які виникають при кратному врахуванні зв’язків симплексів, що пов’язані між собою через дотичні вершини, ребра, грані тощо. Для компенсації надмірності враховується R^*.

Розглянемо приклад обрахунків ризиків із урахуванням структури системи на узагальненому прикладі. Припустимо, що маємо структуру систему у вигляді, представленому на рисунку 3.2.

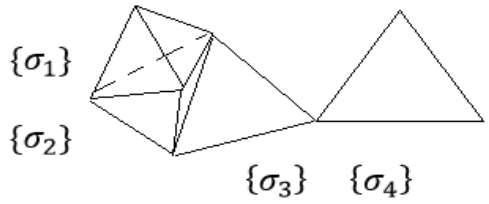


Рисунок 3.2 – Симплеціальний комплекс для структури системи

У цьому випадку $\{\sigma_1\}$, $\{\sigma_2\}$, $\{\sigma_3\}$, $\{\sigma_4\}$ – симплекси, з яких складається комплекс структури системи. Кожний з них складається з елементів, які його породжують, а також зв'язків різної арності.

$\{\sigma_1\}$ – складається з чотирьох елементів, назвемо їх e_1, e_2, e_3, e_4, які зв'язані між собою зв'язками третього рівня, тобто кожний з них одночасно зв'язаний з іншими й одночасно утворюють просторовий зв'язок у вигляді тетраедра.

$\{\sigma_2\}$ має аналогічну структуру, складається з e_5, e_2, e_3, e_4. Між собою ці симплекси зв'язані через симплекс другого порядку, тобто трикутника з вершинами e_2, e_3, e_4.

$\{\sigma_3\}$ представляє симплекс розмірності 2, складається з елементів e_4, e_5, e_6. Через одномірний зв'язок, що складається з e_4, e_5, $\{\sigma_3\}$, він зв'язаний з $\{\sigma_2\}$.

Останнім елементом комплексу є $\{\sigma_4\}$, який складається з e_7, e_8, e_6. Він пов'язаний через 0-мірний зв'язок e_6 з $\{\sigma_3\}$.

Для того, щоб коректно обрахувати рівень ризику, необхідні дані для обрахунку $R_{\sigma_1}, R_{\sigma_2}, R_{\sigma_3}, R_{\sigma_4}$, а також R_{e_2,e_3,e_4}, R_{e_4,e_5}, R_{e_6}.

Остаточні значення розраховуються як ризики відповідних симплексів, тому мають певні особливості.

Припустимо, що для нашого прикладу маємо всі необхідні дані. У цьому випадку, загальний вигляд формули оцінки ризику (3.13) буде наступним:

$$R = \sum_{i=1}^{4} R_{\sigma_i} - R_{e_2,e_3,e_4} - R_{e_4,e_5} - R_{e_6}. \quad (3.13)$$

Такий вигляд формули оцінки ризику є більш практичним для застосування, оскільки враховує специфіку структури системи, та дозволяє досягнути більш точного рівня оцінки. Слід зауважити, що у разі, коли через наявні симплекси q-зв'язку, які визначаються через їх вершини, одночасно зв'язуються більше ніж два симплекси, то вони мають помножуватися на коефіцієнт m-1, де m кількість симплексів, які зв'язані через цей q-зв'язок.

Після обрахунку ризиків для кожної підсистеми, елемента та здійснення загальної оцінки ризику для системи в цілому, можна зробити висновки про те, як кожна окрема вразливість впливає на загальний ризик системи в цілому.

Запропонований підхід дозволяє більш ефективно визначити та ранжувати пріоритети перед вирішенням задач, пов'язаних із забезпеченням кібербезпеки. Перевага такого підходу полягає в тому, що він є більш виваженим та структурно обґрунтованим, ніж звичайна матриця ризиків.

Для обрахунків наведених ризиків застосовується Q-аналіз. Використання оберненої задачі надає можливість побудувати симплеціальний комплекс. Пряма задача дозволяє оцінити пріоритет вразливостей. Здійснення відповідного аналізу дозволяє провести ймовірнісний розподіл в системі вразливостей. Останнє може стати у нагоді у разі, коли статистичний розподіл виникнення вразливостей та загроз не встановлено.

При цьому, слід урахувати, що показник, який характеризує потенційні збитки та втрати, залишається достатньо суб'єктивним через складний механізм отримання достовірної інформації, оскільки вона інколи носить конфіденційний характер та часто базується на експертних оцінках фахівців. Останнє вимагає проведення додаткових досліджень у напрямку забезпечення належного рівня кібербезпеки системи із застосовуванням сценаріїв розвитку подій, які реалізують уразливості внаслідок здійснення несанкціонованого вторгнення – хакерської атаки на інформаційну систему.

3.3 Узагальнений метод розрахунку оцінки ризиків

Узагальнюючи всі підходи, які опрацьовані під час проведення дисертаційного дослідження, нижче наводимо повний метод розрахунку оцінки ризиків для систем складної структури. У рамках дослідження зроблено припущення, що будь-яка система вразливостей має складну структуру, що обумовлено наявними та потенційними загрозами для кіберсистеми.

Наведемо всі етапи отриманого узагальненого методу.

І етап. Збір даних про структуру вразливостей та загроз системи.

Виходячи з наявної інформації, визначаються зв'язки та залежності між загрозами та вразливостями системи, формується відповідна матриця інцидентності. Дані можуть бути представлені у вигляді структурного графу (симлеціального комплексу), звичайного графу або у вигляді опису закономірностей взаємодії між елементами.

ІІ етап. Синтез симплеціального комплексу.

Застосовується методика побудови симплеціального комплексу системи за допомогою матриці інцидентності, яка наведена у розділі 2.

ІІІ етап. Використання методів Q-аналізу для виявлення структурних особливостей симплеціального комплексу.

Здійснюється побудова структурного дерева, локальних карт та ієрархії нащадків. Їх характеристики використовуються на наступних етапах методики.

IV етап. Класифікація загроз/вразливостей в комплексі на основі Q-аналізу.

На основі виявлених структурних особливостей системи таких, як q-зв'язок, q-зв'язність та ієрархія нащадків проводиться класифікація загроз/вразливостей в симплеціальному комплексі. Цю класифікацію можна використовувати замість порядкової шкали, наприклад, як рівень критичності загрози/вразливості за відсутності достовірних оцінок.

V етап. Визначення розподілу ймовірностей та рівня втрат.

Виходячи з профілю атак на кіберсистему, формується розподіл ймовірностей для загроз. За допомогою експертних методів визначаються оцінки втрат від уразливостей і загроз у залежності від їх комбінації.

VI етап. Розрахунок оцінок ризиків для кіберсистеми.

Згортання структурного дерева. На основі локальних карт та структурного графу синтезується формула для розрахунку загального ризику системи.

Використовуючи локальні карти та структурне дерево, будуємо формулу розрахунку загального ризику системи:

- для кожного листка дерева на будь-якому рівні зв'язності обраховуються ризики для відповідного симплексу (кожен ризик є частковим, але розрахунок його не тривіальний);
- при русі по структурному дереву призводить до того, що окремі симплекси зв'язуються в ланцюги, тобто відбувається «склеювання» симплексів з різною ступеню q-зв'язку.

У формулі загального ризику системи поправка на склейки виглядає як віднімання деякої величини ризику, порахованого по цій склейці. Тобто якщо два симплекса розмірності 3, склеєні через симплекс розмірності 2, тоді потрібно порахувати окремо ризики для кожного з симплексів, додати між собою ризики для симплексів, що склеюються та відняти величину ризику по склейці. Це потрібно для того, щоб не враховувати ризики по склейці двічі. Формула, що описує цей підхід наведена в розділі 3.

Пройшовши все структурне дерево і використавши складені функції втрат та структурну формулу оцінки ризику, отримуємо узагальнений вигляд формули розрахунку оцінки ризику для кіберсистем складної структури.

Уточнимо, що цей підхід для обрахунку будь-якої адитивної міри носить об'єктивний характер у разі, коли він вкладається в терміни структурного дерева і локальних карт. Тому цей метод має достатньо широке застосування, і може застосовуватися не лише для здійснення оцінки кіберсистем та вразливостей, а і для будь-якої складної за структурою системи, якщо він

включає в себе процедуру синтезу комплексу системи з урахуванням «включення-виключення» внесків (впливів) від різних компонент.

Висновки до розділу 3

У цьому розділі описано новий узагальнений метод оцінки ризиків для систем складної структури. Розглянуто різні варіанти розрахунку функції середнього ризику системи у залежності від сумісності реалізації структурних компонентів загроз.

Наведено формулу розрахунку функції втрат з урахуванням ймовірнісних характеристик сумісної реалізації вразливостей подій у системі.

Запропоновано обчислення ризику здійснювати для комплексу в цілому за адитивною формулою з поправками на надмірність унаслідок кратності склеювання між симплексами.

Запропоновано метод побудови формули байєсової оцінки ризику з урахуванням структури симплеціального комплексу, створеного на основі системи зв’язків між уразливостями та загрозами.

Запропонована формула має поліноміальний вигляд, що обумовлено сумісністю загроз та профілем атак. При цьому, не зважаючи на вищенаведене, вона дозволяє достатньо просто здійснювати аналітичні дослідження для виявлення максимального та мінімального ризику, а також умов, при яких може виникати високий рівень поправки на «склейки».

Апробацію узагальненого методу оцінки ризиків для систем складної структури здійснено на прикладі розрахунку оцінки ризику для інформаційної системи критичної інфраструктури, характеристики (вхідні дані) якої наведено у розділі 4.

РОЗДІЛ 4

ПРИКЛАД ОЦІНКИ РИЗИКУ ДЛЯ ВИБРАНОЇ КІБЕРСИСТЕМИ

4.1 Опис даних для оцінки ризику для інформаційної системи об’єкта критичної інфраструктури

У попередніх розділах було наведено методологію розширеного Q-аналізу оцінки ризиків на основі взаємозалежності між загрозами та вразливостями кібернетичних систем, а також специфіку його застосування при оцінці ризику та побудові функцій втрат. В цьому розділі наведено наукові підходи щодо практичного застосування отриманих теоретичних результатів та їх використання в реальних системах.

Попереднім етапом є збір даних та представлення її в тому вигляді, який є необхідним для застосування методології.

У залежності від характеристик зібраної інформації передбачається декілька варіантів її первинної обробки.

Перший випадок вважається найкращим, але практично не зустрічається. Це випадок, коли дані вже представлені у вигляді структурної залежності, тобто у формі симлеціального комплексу.

Другий випадок є більш ймовірним. Це випадок, коли зібрані первинні дані представлені у вигляд матриці інцидентності між уразливостями та загрозами. У такому вигляді зібрані дані інколи зустрічаються.

Третій випадок є найбільш поширеним. Зібрані дані носять конфіденційний характер, або вони є достаньмо специфічними з вузькою предметною сферою застосування. У цьому випадку доцільно використовувати обернені задачі Q-аналізу для побудови симплеціального комплексу з метою проведення подальшого аналізу.

Для проведення дослідження практичного застосування методології розширеного Q-аналізу, у рамках дисертаційного дослідження, використано дані системи загроз і вразливостей інформаційної системи об’єкта критичної інфраструктури (далі – ІСОКІ), наведеного в роботі В. Куза [86].

Уразливості, використані для проведення дослідження, а також оцінювання визначеного переліку загроз $\{u_k\}$ для умовного об'єкта критичної інфраструктури отримані у результаті експертного аналізу ІСОКІ. За результатами проведеного експертного аналізу сформовано також перелік $\{b_l\}$, $l = \{1, 2, ..., L\}$ елементів, які позначають уразливості. Останні взаємопов'язано із потенційно вразливими компонентами, на які саме і можуть бути спрямовані кібератаки.

Для зазначеної ІСОКІ сформовано наступний перелік елементів, які характеризують уразливості:

b_1 – уразливість вхідних драйверів вхідної інформації;

b_2 – уразливість драйверів відображення інформації;

b_3 – уразливість драйверів інструментів обробки інформації;

b_4 – уразливість драйверів мікросхем BIOS;

b_5 – уразливість програмного забезпечення серверів з відкритим фізичним доступом;

b_6 – уразливість програмного забезпечення комунікаційного обладнання об'єкта;

b_7 – уразливість стеку протоколів TCP/IP;

b_8 – уразливість шлюзу входу в Інтернет;

b_9 – уразливість протоколів прикладного рівня міжмережевої взаємодії;

b_{10} – уразливість не задокументованих точок міжмережевої взаємодії;

b_{11} – уразливість відкритих спільних мережевих ресурсів;

b_{12} – уразливість не сертифікованих програмних компонентів;

b_{13} – уразливість електронної пошти;

b_{14} – уразливість веб-браузера;

b_{15} – уразливість кабелів обладнання об'єкта на місцях, де є вільний фізичний доступ до них.

Визначений перелік загроз від кібератак для ІСОКІ наведено нижче:

u_1 – загроза завантаження шкідливого (вірусного) програмного забезпечення, використовуючи особливості альтернативної операційної системи з розширеними повноваженнями;

u_2 – загроза несанкціоноване копіювання інформації;

u_3 – загроза неавторизованої модифікації інформації;

u_4 – загроза реалізації помилкової авторизації об'єкта;

u_5 – загроза неконтрольованої, не задокументованої заміни системного програмного забезпечення;

u_6 – загроза пере направлення мережевого трафіку;

u_7 – загроза маніпулювання даними у віддаленому режимі;

u_8 – загроза злому електронної поштової скриньки;

u_9 – загроза блокування електронної скриньки;

u_{10} – загроза заміни веб-браузерів;

u_{11} – загроза системної помилки при використанні прикладного програмного забезпечення;

u_{12} – загроза блокування хосту користувача;

u_{13} – загроза блокування роутера;

u_{14} – загроза обходу брандмауера.

4.2 Практичне застосування методу оцінки ризиків на основі структурного Q-аналізу

Згідно з методологією розширеного Q-аналізу, використовуючи наведені вище переліки елементів, які позначають уразливості, та загроз від кібератак, побудовано матрицю інцидентності (q-зв'язності) між уразливостями та загрозами ICOKI (таблиця 4.1).

Таблиця 4.1 – Матриця інцидентності між уразливостями та загрозами для ІСОКІ

	Уразливість інформаційних ресурсів ІСОКІ до реалізації загроз комп’ютерних атак														
Загрози комп'ютерних атак	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9	b_{10}	b_{11}	b_{12}	b_{13}	b_{14}	b_{15}
u_1	1	0	0	0	1	1	0	0	0	0	0	1	1	1	1
u_2	0	0	0	0	1	0	0	1	1	1	1	1	1	1	1
u_3	1	1	1	0	1	0	0	1	1	1	1	1	1	1	1
u_4	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1
u_5	1	1	1	0	0	0	0	0	0	0	0	0	1	1	1
u_6	1	1	1	0	1	1	1	1	1	1	0	0	1	1	1
u_7	1	1	1	0	0	0	1	0	0	0	0	0	1	0	0
u_8	1	1	1	0	0	1	0	0	1	0	0	0	1	1	0
u_9	1	1	1	0	0	1	0	0	1	0	0	0	1	1	0
u_{10}	1	1	1	0	0	1	0	0	1	0	0	0	1	0	1
u_{11}	1	1	0	0	0	0	0	0	0	0	1	0	1	0	0
u_{12}	1	0	0	0	0	1	0	1	0	0	0	1	0	0	0
u_{13}	1	0	0	0	0	1	0	1	0	1	1	1	0	0	0
u_{14}	1	1	1	0	0	0	0	0	0	0	0	0	1	0	0

Наступним кроком є побудова матриці q-зв’язності для системи загроз у залежності від уразливостей b_{i}, яка наведена у таблиці 4.2.

Таблиця 4.2 – Матриця симплеціального комплексу для системи загроз в залежності від вразливостей

Загрози	u_1	u_2	u_3	u_4	u_5	u_6	u_7	u_8	u_9	u_{10}	u_{11}	u_{12}	u_{13}	u_{14}
u_1	7	5	6	7	4	6	2	4	4	4	2	3	3	2
u_2	5	9	9	9	3	7	1	3	3	3	2	2	4	1
u_3	6	9	12	12	6	10	4	6	6	6	4	3	5	4
u_4	7	9	12	14	6	12	5	7	7	7	4	4	6	4
u_5	4	3	6	6	6	6	4	5	5	5	3	1	1	4
u_6	6	7	10	12	6	12	5	7	7	7	3	3	4	4
u_7	2	1	4	5	4	5	5	4	4	4	3	1	1	4
u_8	4	3	6	7	5	7	4	7	7	6	3	2	2	4
u_9	4	3	6	7	5	7	4	7	7	6	3	2	2	4
u_{10}	4	3	6	7	5	7	4	6	6	7	3	2	2	4
u_{11}	2	2	4	4	3	3	3	3	3	3	4	1	2	3
u_{12}	3	2	3	4	1	3	1	2	2	2	1	4	4	1
u_{13}	3	4	5	6	1	4	1	2	2	2	2	4	6	1
u_{14}	2	1	4	4	4	4	4	4	4	4	3	1	1	4

Наступний етап – проведення структурного Q-аналізу для виявлення можливих сумісних реалізацій уразливостей, які проявляються через складну структуру взаємозалежностей між уразливостями та загрозами. На основі розроблених та представлених у другому розділі алгоритмів, будуємо локальні карти та структурне дерево, які наведені нижче на рисунку 4.1 та рисунку 4.2.

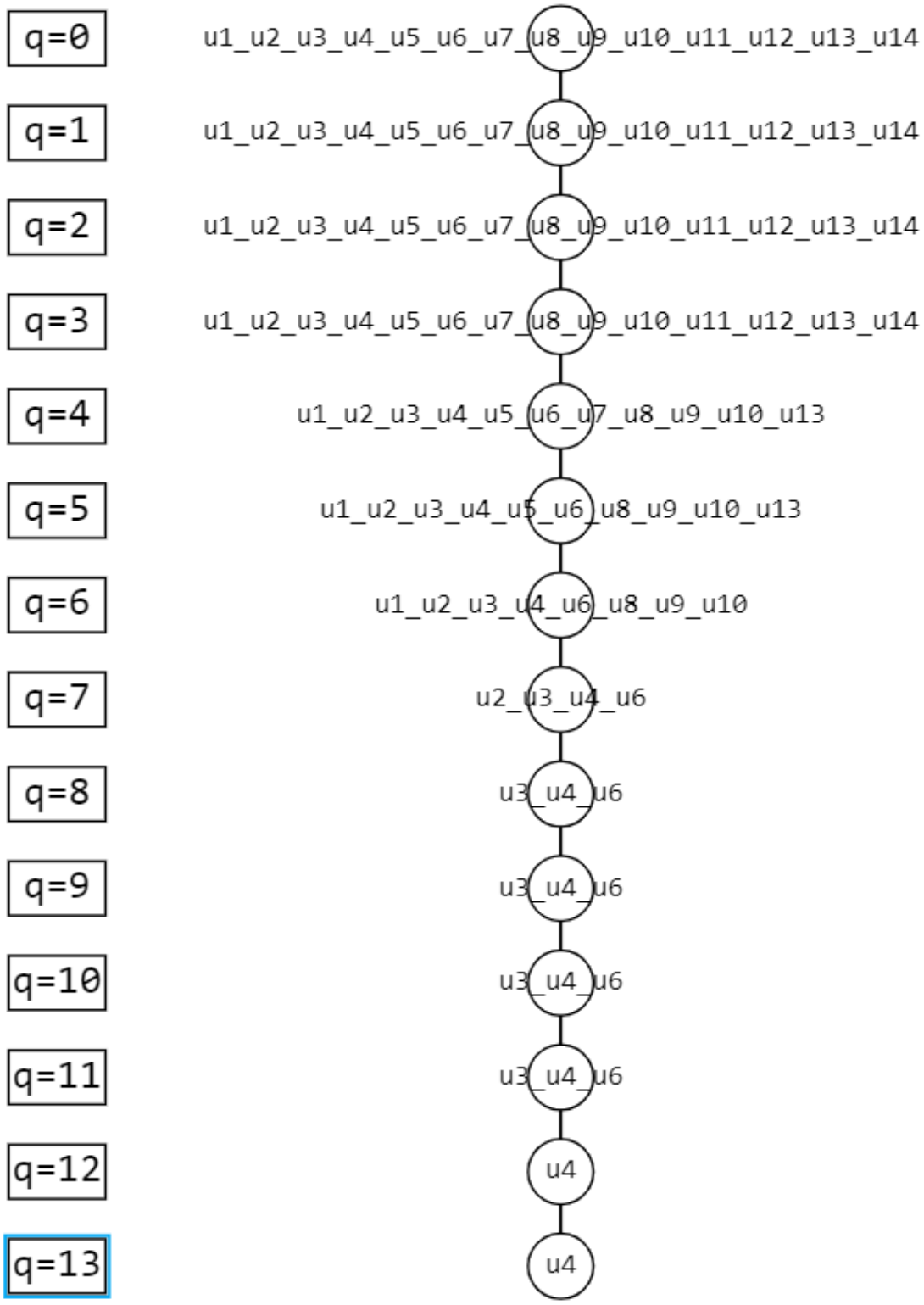


Рисунок 4.1 - Структурне дерево

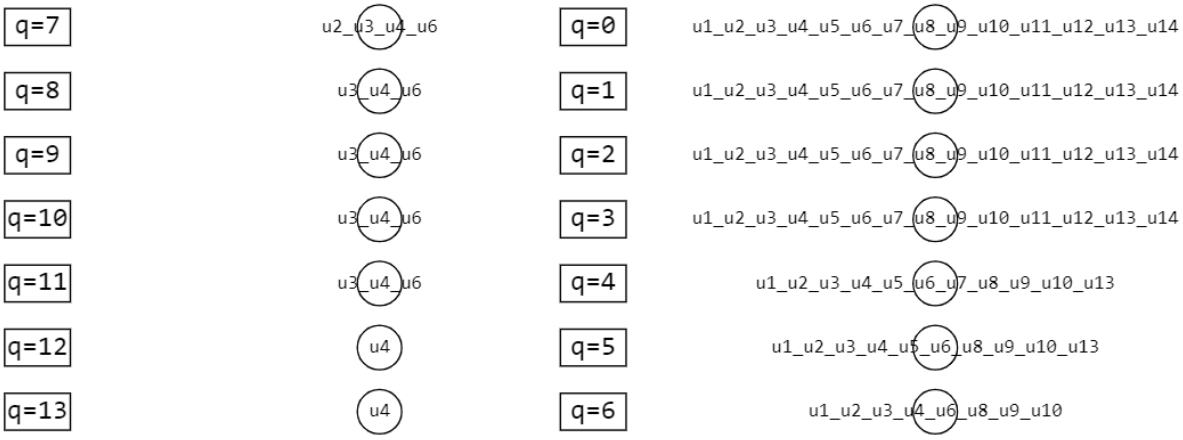


Рисунок 4.2 - Локальні карти

Наступним етапом є проведення класифікації вразливостей з урахуванням вимог та параметрів, наведених у розділі 2.

Спочатку класифікуємо вразливості за ступенем зв'язності. Визначаємо наскільки взаємозалежна або сумісна визначена загроза з іншими. Нижче наведено характеристики загроз для проведення відповідної оцінки.

Загрози u_{11}, u_{12}, u_{14} є структурними частинами ланцюга на рівні зв'язності q=0-3, тому не виокремлюються в окремі симплекси та мають низьку сумісність з іншими загрозами, а також не значну залежність від уразливостей.

Загроза u_7 є структурним елементом ланцюга рівня зв'язності q=5. У подальшому не виокремлюється в окремі симплекси, але через те, що викликається малою кількістю вразливостей, на рівні зв'язності 5 вже не відображається.

Загрози u_5 і u_{13} є структурними елементами ланцюга до рівня зв'язності q=4. У подальшому не виокремлюються в окремі симплекси, але через те, що викликаються малою кількістю вразливостей, на рівні зв'язності 4 вже не відображаються.

Загрози u_1, u_8, u_9, u_{10} є структурними елементами в ланцюзі разом з іншими вразливостями до рівня зв'язності q=7, при цьому, мають ще й велику залежність від кількості вразливостей.

Загроза u_2 є структурним елементом в ланцюзі з іншими вразливостями до рівня зв'язності q=8, тобто має ще й велику залежність від кількості вразливостей.

Загрози u_3, u_6 є структурними елементами в ланцюзі з іншими вразливостями до рівня зв'язності q=11, тобто мають ще й великий вплив на виникнення загроз.

Загроза u_4 є структурним елементом в ланцюзі з іншими вразливостями до рівня зв'язності q=11, далі виокремлюється в окремий симплекс. Це означає, що ця загроза має найбільшу залежність від уразливостей.

Наступним кроком є проведення класифікації загроз за розмірністю примикання. В основу цієї класифікації покладено визначення максимального ступеню зв'язку між симплексами. Характеристики загроз за цією класифікацією наведено нижче.

На рівні зв'язності q=0 – всі загрози мають сумісну реалізацію і примикання між собою.

На рівні зв'язності q=1-3 – всі загрози мають сумісну реалізацію і примикання між собою. При цьому, зникають окремі зв'язки між ними, але в цілому симплекси примикають один до одного з різним ступенем q-зв'язку.

На рівні зв'язності q=4 – загрози u_{11}, u_{12}, u_{14} повністю вбудовані в комплекс, але через їх низький вплив на рівень безпеки, на цьому рівні вже не відображаються.

На рівні зв'язності q=5 – загроза u_7 має таку ж саму характеристику: повністю вбудована в комплекс, але має дещо більшу залежність від уразливостей.

На рівні зв'язності q=6 – загрози u_5, u_{13} мають таку ж характеристику: повністю вбудовані в комплекс, але мають ще більшу залежність від уразливостей.

На рівні зв'язності q=7 – загрози u_1, u_8, u_9, u_{10} мають таку ж характеристику: повністю вбудовані в комплекс, але мають ще більш високу залежність від уразливостей.

На рівні зв’язності q=8 – загроза u_2 має таку ж характеристику: повністю вбудована в комплекс, але має ще більш високу залежність від уразливостей.

На рівні зв’язності q=9 – q=12 – загрози u_3, u_6 повністю будовані в ланцюг, тому не виділяються у окремі симплекси. Вони мають таку ж характеристику, як і в попередніх випадках: повністю вбудовані в комплекс, але мають ще більшу залежність від уразливостей.

На рівні зв’язності q=13 – загроза u_4 має найбільший вплив майже на всі загрози в системі, тому й має найбільшу комбінацію залежностей від уразливостей.

Наступним кроком є проведення класифікації за кількістю нащадків. В основу цієї класифікації покладено визначення сумісності певної загрози з іншими. Виходячи зі структурного дерева, на основі цієї класифікації маємо відповідні характеристики загроз.

Загроза u_4 має одного нащадка, але великої розмірності q=12.

Усі інші загрози не мають нащадків, бо не виокремлюються в симплекси, а є структурними елементами ланцюгів симплексів.

Для кращого відображення зв’язків між загрозами, побудовано структурні графи на кожному рівні q-зв’язку, які наведено нижче на рисунках 4.3 – 4.10.

Графічне відображення зв’язків дозволяє більш адекватно прорахувати ризик на кожному рівні зв’язку між загрозами. Адже на локальних картах не відображаються різні рівні зв’язку між загрозами, особливо, коли деякі симплекси є структурними елементами інших симплексів більш високої розмірності.

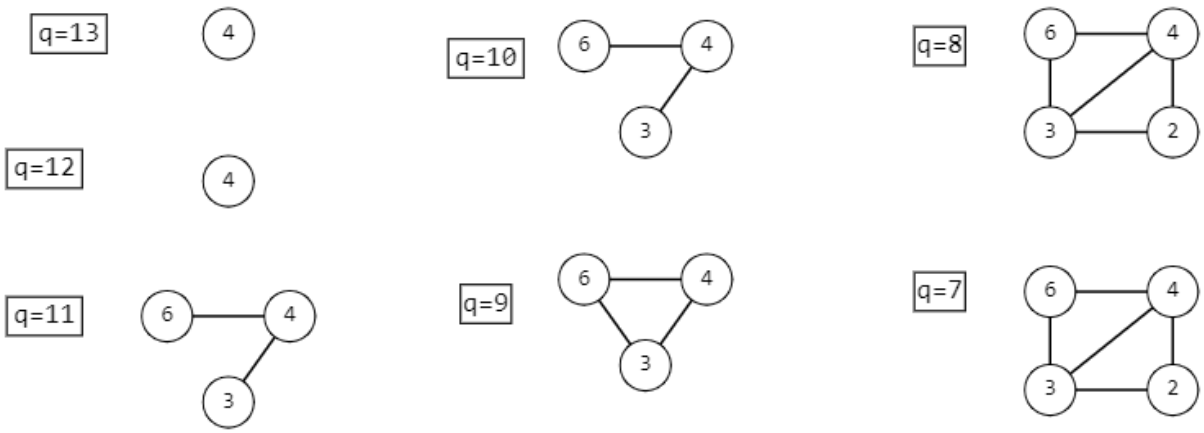


Рисунок 4.3 – Структурні графи на рівнях q=13, q=12, q=11, q=10, q=9, q=8, q=7

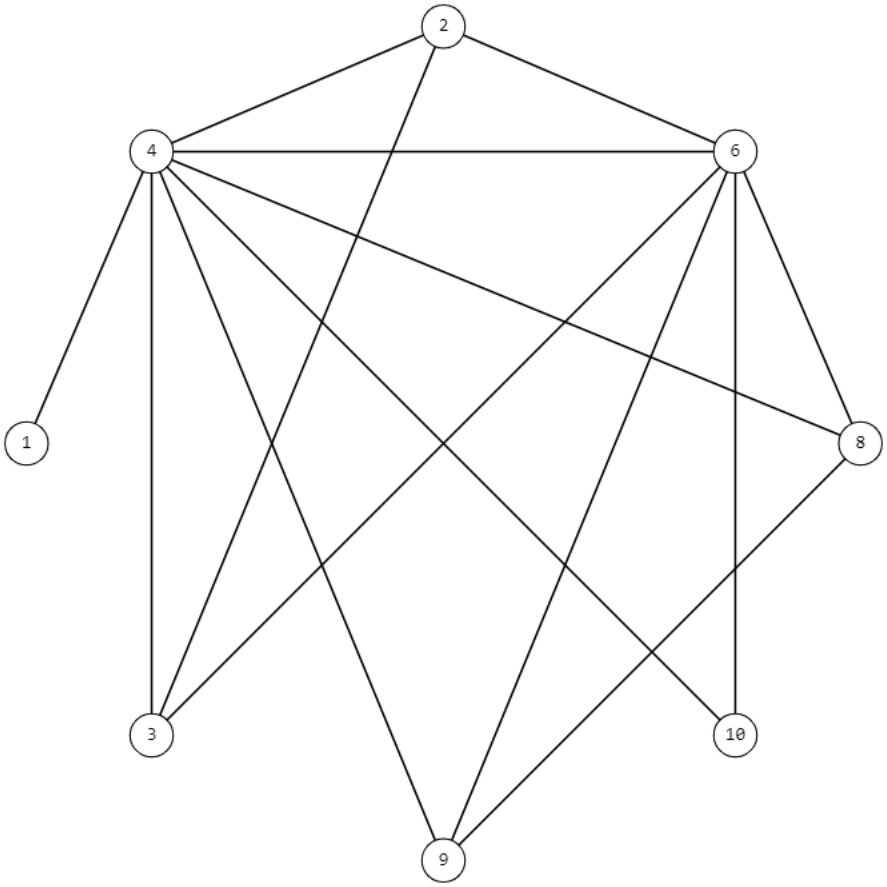


Рисунок 4.4 – Структурний граф на рівні q=6

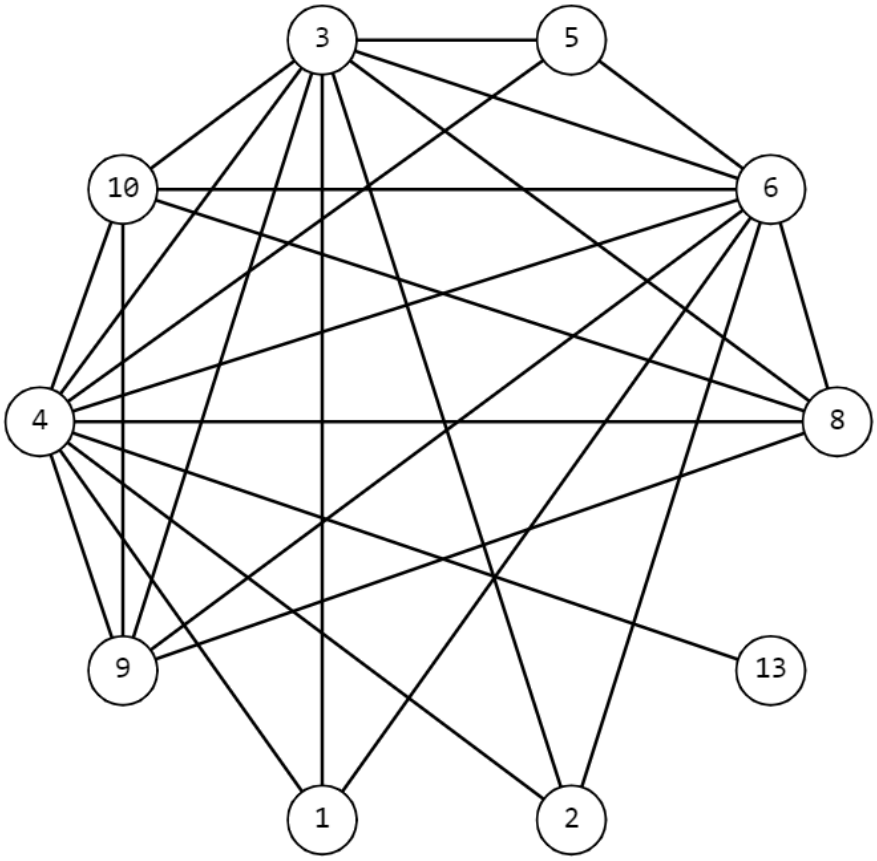


Рисунок 4.5 – Структурний граф на рівні q=5

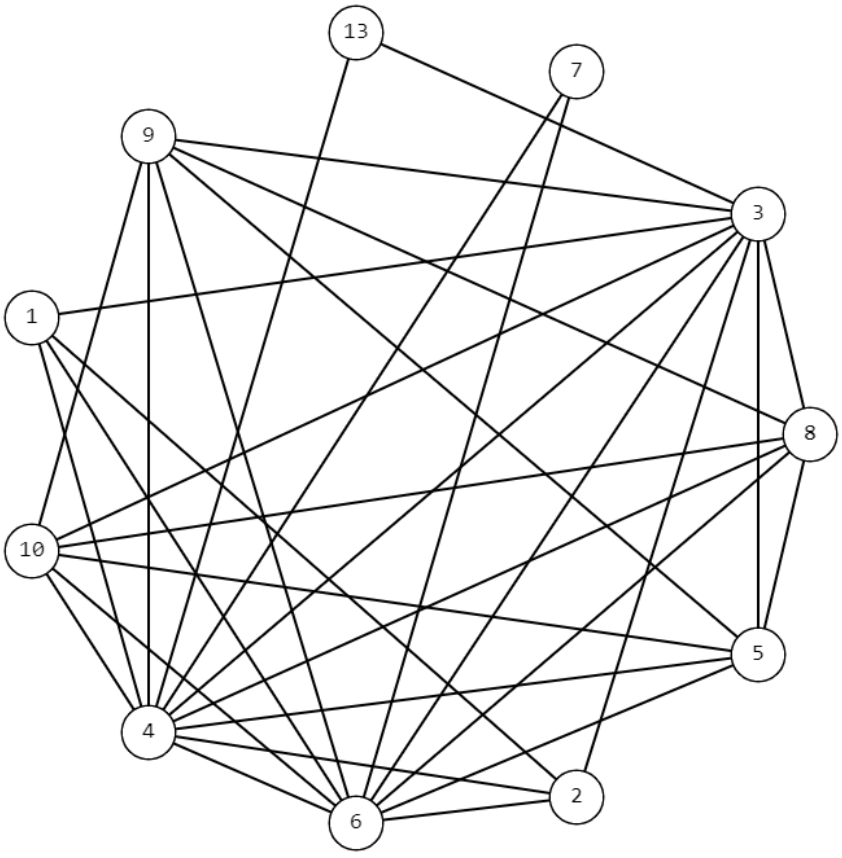


Рисунок 4.6 – Структурний граф на рівні q=4

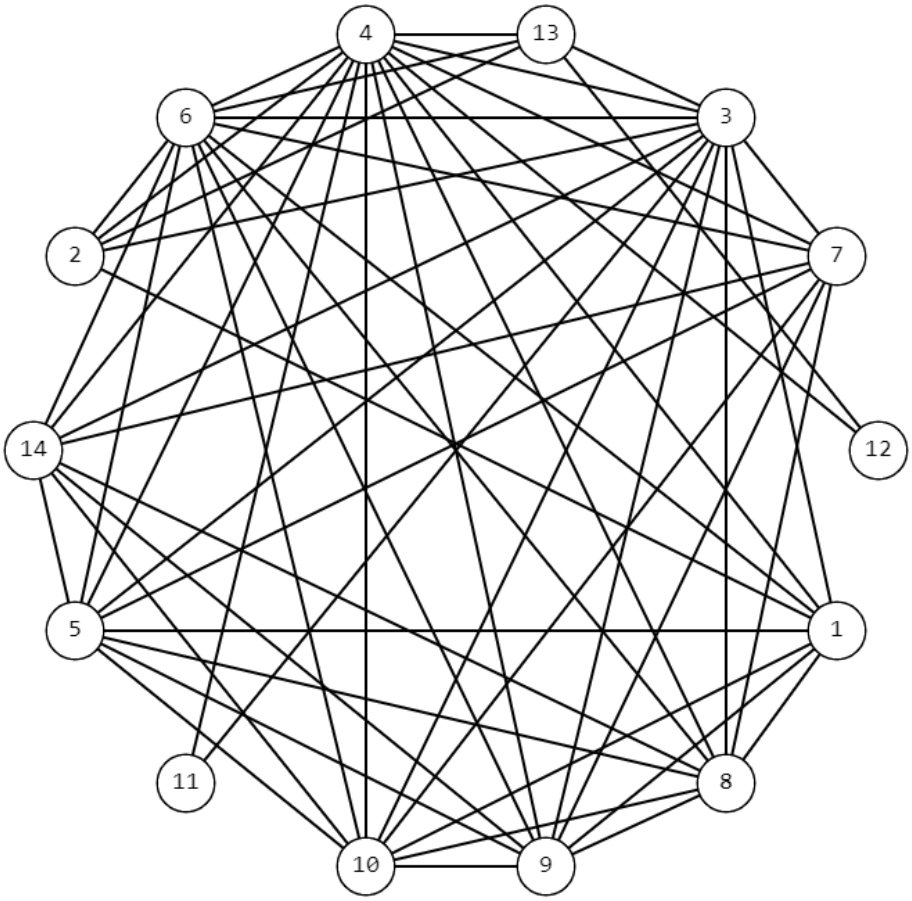


Рисунок 4.7 – Структурний граф на рівні q=3

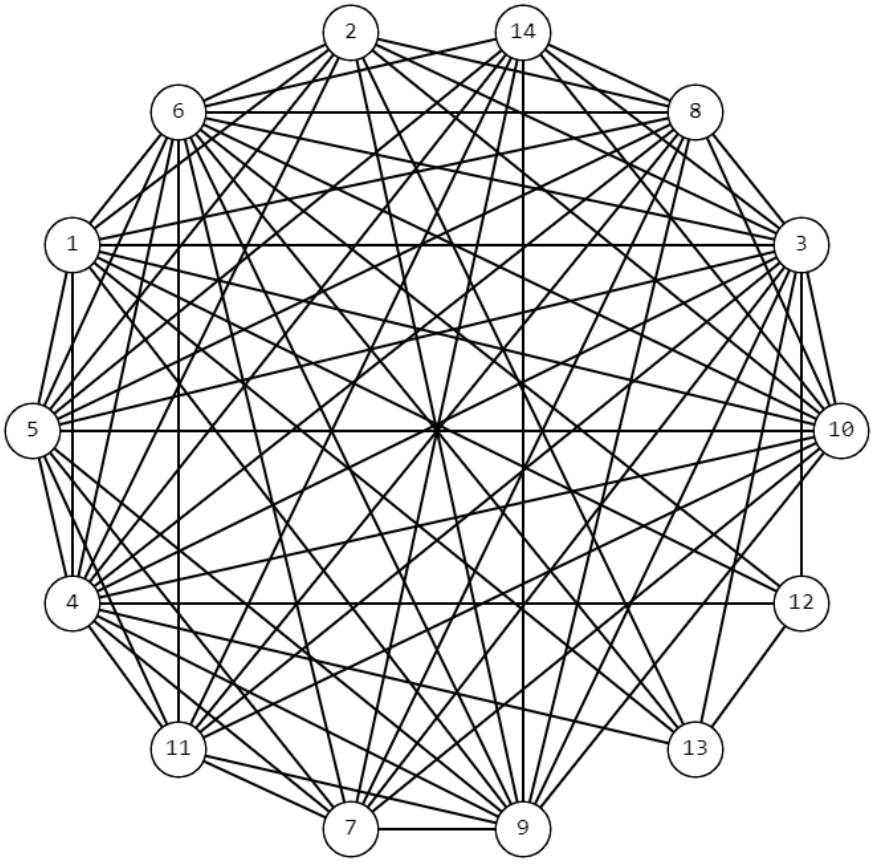


Рисунок 4.8 – Структурний граф на рівні q=2

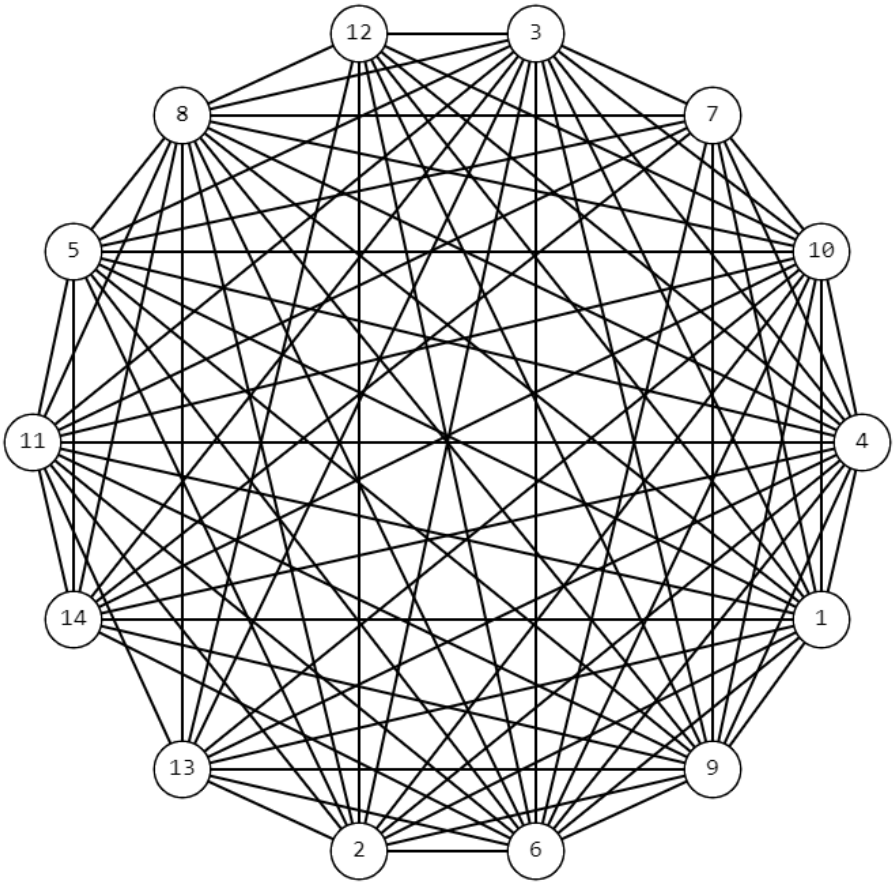


Рисунок 4.9 – Структурний граф на рівні q=1

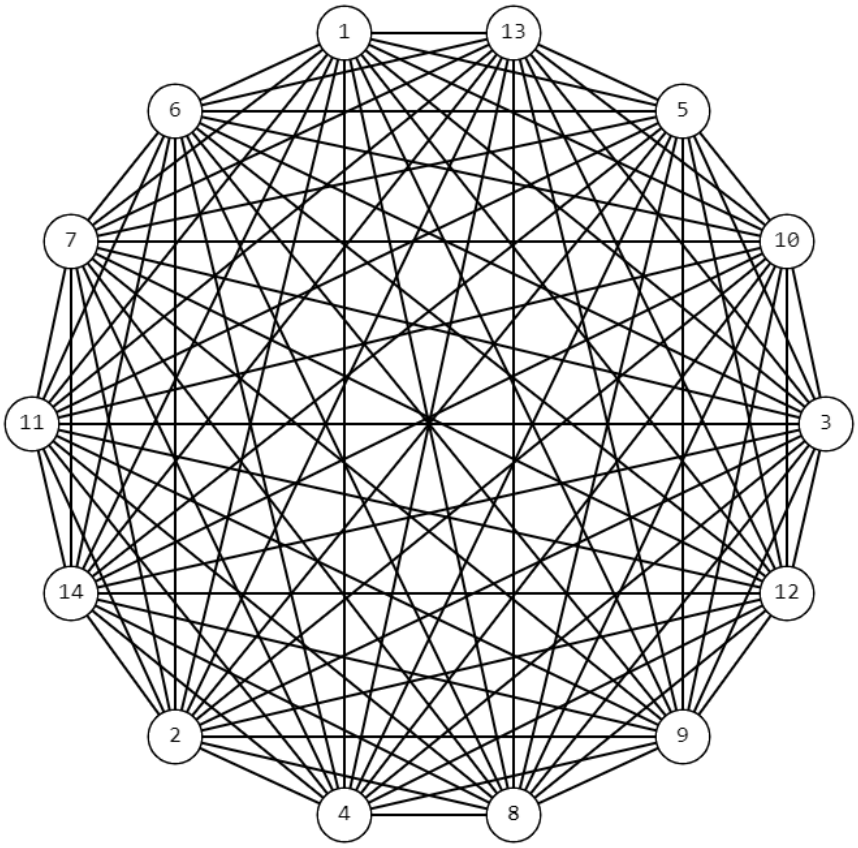


Рисунок 4.10 – Структурний граф на рівні q=0

Після виявлення рівнів критичності загроз, наступним кроком є проведення оцінки ризиків із застосуванням узагальненого методу оцінки кіберризиків на основі складної структури загроз, який наведено в розділі 3.

Виходячи зі структури досліджуваної ІСОКІ, формули оцінки ризиків виглядатиме на різних рівнях q-зв'язку наступним чином.

На рівні зв'язності q=13 ризик розраховується через уразливості, які залежать загрози від u_4, за формулою (4.1):

$$R_{u4} = \sum_{i=1}^{15/4} R_{b_i} + \sum_{i=1, i\neq j}^{15/4} R_{b_{\{i,j\}}} + \sum_{i=1, i\neq j\neq k}^{15/4} R_{b_{\{i,j,k\}}} + \cdots + R_{b_{\{i,j,k,\ldots,z\}}} \quad (4.1)$$

На рівні зв'язності q=12 ризик розраховується за формулою (4.1).

На рівні зв'язності q=11 ризики розраховуються через уразливості, що залежать від загроз u_3, u_4, u_6, з поправкою на примикання за формулами (4.2) – (4.5).

$$R_{u3} = \sum_{i=1}^{15/4,6,7} R_{b_i} + \sum_{i=1, i\neq j}^{15/4,6,7} R_{b_{\{i,j\}}} + \sum_{i=1, i\neq j\neq k}^{15/4,6,7} R_{b_{\{i,j,k\}}} + \cdots + R_{b_{\{i,j,k,\ldots,z\}}} \quad (4.2)$$

$$R_{u6} = \sum_{i=1}^{15/4,11,12} R_{b_i} + \sum_{i=1, i\neq j}^{15/4} R_{b_{\{i,j\}}} + \sum_{i=1, i\neq j\neq k}^{15/4} R_{b_{\{i,j,k\}}} + \cdots + R_{b_{\{i,j,k,\ldots,z\}}} \quad (4.3)$$

$$R_{\{u3,u4\}} = R_{b1,b2,b3,b5,b8,b9,b10,b11,b12,b13,b14,b15} = R_{b_{\{3,5,8,9,10,11,12,13,14,15\}}} = \sum_{i=1}^{\{3,5,8,9,10,11,12,13,14,15\}} R_{b_i} + \sum_{i=1, i\neq j}^{\{3,5,8,9,10,11,12,13,14,15\}} R_{b_{\{i,j\}}} + \sum_{i=1, i\neq j\neq k}^{\{3,5,8,9,10,11,12,13,14,15\}} R_{b_{\{i,j,k\}}} + \cdots + R_{b_{\{3,5,8,9,10,11,12,13,14,15\}}} \quad (4.3)$$

$$R_{\{u6,u4\}} = R_{b1,b2,b3,b5,b6,b7,b8,b9,b10,b13,b14,b15} = R_{b_{\{3,5,6,7,8,9,10,13,14,15\}}} = \sum_{i=1}^{\{3,5,6,7,8,9,10,13,14,15\}} R_{b_i} + \sum_{i=1, i\neq j}^{\{3,5,6,7,8,9,10,13,14,15\}} R_{b_{\{i,j\}}} + \sum_{i=1, i\neq j\neq k}^{\{3,5,6,7,8,9,10,13,14,15\}} R_{b_{\{i,j,k\}}} + \cdots + R_{b_{\{3,5,6,7,8,9,10,13,14,15\}}}, \quad (4.4)$$

де $R_{\{u3,u4\}}$, $R_{\{u6,u4\}}$ – ризик прорахований для «склейки».

$$R_{u3,u4,u6} = R_{u3} + R_{u4} + R_{u6} - R_{\{u6,u4\}} - R_{\{u3,u4\}}, \quad (4.5)$$

де $R_{u3,u4,u6}$ – загальний ризик на відповідному рівні.

На рівні зв'язності q=10 ризик розраховується на основі формули, наведеної вище через уразливості, що залежать від загроз u_3, u_4, u_6 з поправкою на примикання.

На рівні зв'язності q=9 ризик розраховується на основі формули, наведеної вище через уразливості, що залежать від загроз u_3, u_4, u_6 з поправкою на примикання При цьому, виникає додатковий зв'язок $R_{\{u3,u6\}}$, але він урахований на попередньому етапі склейки.

На рівні зв'язності q=8 ризик розраховується на основі формули, наведеної вище через уразливості, що залежать від загроз u_3, u_4, u_6 з поправкою на примикання.

На рівні зв'язності q=7 ризик розраховується через уразливості, що залежать від загроз u_2, u_3, u_4, u_6 з поправками на примикання.

Розрахунок ризиків для цього рівня зв'язності здійснюється за формулами (4.6) – (4.8).

$$R_{u2} = \sum_{i=5}^{\{8,9,10,11,12,13,14,15\}} R_{b_i} + \sum_{i=5,i\neq j}^{\{8,9,10,11,12,13,14,15\}} R_{b_{\{i,j\}}} + \\ + \sum_{i=5,i\neq j\neq k}^{\{8,9,10,11,12,13,14,15\}} R_{b_{\{i,j,k\}}} + \cdots + R_{b_{\{5,8,9,10,11,12,13,14,15\}}} \quad (4.6)$$

$$R_{\{u2,u3\}} = R_{b5,b8,b9,b10,b11,b12,b13,b14,b15} = \\ = \sum_{i=5}^{\{8,9,10,11,12,13,14,15\}} R_{b_i} + \sum_{i=5,i\neq j}^{\{8,9,10,11,12,13,14,15\}} R_{b_{\{i,j\}}} + \\ + \sum_{i=5,i\neq j\neq k}^{\{8,9,10,11,12,13,14,15\}} R_{b_{\{i,j,k\}}} + \cdots + R_{b_{\{5,8,9,10,11,12,13,14,15\}}} \quad (4.7)$$

$$R_{\{u2,u6\}} = R_{b5,b8,b9,b10,b13,b14,b15} = \\ = \sum_{i=5}^{\{8,9,10,11,14,15\}} R_{b_i} + \sum_{i=5,i\neq j}^{\{8,9,10,13,14,15\}} R_{b_{\{i,j\}}} + + \sum_{i=5,i\neq j\neq k}^{\{8,9,10,13,14,15\}} R_{b_{\{i,j,k\}}} \\ + \cdots + R_{b_{\{5,8,9,10,13,14,15\}}} \quad (4.8)$$

Зауважимо, що ризик $R_{\{u2,u6\}}$ повністю охоплює ризик $R_{\{u2,u3\}}$, тому додатково враховувати його не потрібно.

Нижче наведено загальну формулу розрахунку ризику для цього рівня зв'язності (4.9).

$$R_{u2,u3,u4,u6} = R_{u2} + R_{u3} + R_{u4} + R_{u6} - R_{\{u6,u4\}} - R_{\{u3,u4\}} - R_{\{u2,u3\}} \quad (4.9)$$

На рівні зв'язності q=6 ризик розраховується через уразливості, що залежать від загроз u_1, u_2, u_3, u_4, u_6, u_8, u_9, u_{10}, із поправками на примикання.

Розрахунок ризиків для цього рівня зв'язності здійснюється за формулами (4.10) – (4.17).

$$R_{u1} = \sum_{i=1}^{\{5,6,12,13,14,15\}} R_{b_i} + \sum_{i=1,i\neq j}^{\{5,6,12,13,14,15\}} R_{b_{\{i,j\}}} + + \sum_{i=1,i\neq j\neq k}^{\{5,6,12,13,14,15\}} R_{b_{\{i,j,k\}}} + \cdots + R_{b_{\{1.5,6,12,13,14,15\}}} \quad (4.10)$$

$$R_{u8} = \sum_{i=1}^{\{2,3,6,9,13,14\}} R_{b_i} + \sum_{i=1,i\neq j}^{\{2,3,6,9,13,14\}} R_{b_{\{i,j\}}} + + \sum_{i=1,i\neq j\neq k}^{\{2,3,6,9,13,14\}} R_{b_{\{i,j,k\}}} + \ldots + R_{b_{\{1,2,3,6,9,13,14\}}} \quad (4.11)$$

$$R_{u9} = \sum_{i=1}^{\{2,3,6,9,13,14\}} R_{b_i} + \sum_{i=1,i\neq j}^{\{2,3,6,9,13,14\}} R_{b_{\{i,j\}}} + + \sum_{i=1,i\neq j\neq k}^{\{2,3,6,9,13,14\}} R_{b_{\{i,j,k\}}} + \ldots + R_{b_{\{1,2,3,6,9,13,14\}}} \quad (4.12)$$

$$R_{u10} = \sum_{i=1}^{\{2,3,6,9,13,15\}} R_{b_i} + \sum_{i=1,i\neq j}^{\{2,3,6,9,13,15\}} R_{b_{\{i,j\}}} + \sum_{i=1,i\neq j\neq k}^{\{2,3,6,9,13,15\}} R_{b_{\{i,j,k\}}} + \ldots + R_{b_{\{1,2,3,6,9,13,15\}}} \quad (4.13)$$

$$R_{\{u1,u4\}} = R_{b1,b5,b6,b12,b13,b14,b15} \quad (4.14)$$

$$R_{\{u4,u8\}} = R_{\{u6,u8\}} = R_{\{u8,u9\}} = R_{b1,b2,b3,b6,b9,b13,b14} \quad (4.15)$$

$$R_{\{u4,u9\}} = R_{b1,b2,b3,b6,b9,b13,b14} \quad (4.16)$$

$$R_{\{u4,u10\}} = R_{\{u6,u10\}} = R_{b1,b2,b3,b6,b9,b13,b15} \quad (4.17)$$

Оскільки окремі склейки дублюються, вони не враховуються. Нижче наведено загальну формулу розрахунку ризику для цього рівня зв'язності (4.18).

$$R_{u1,u2,u3,u4,u6,u8,u9,u10} = R_{u1} + R_{u2} + R_{u3} + R_{u4} + R_{u6} + R_{u8} +$$

$$+R_{u9} + R_{u10} - R_{\{u6,u4\}} - R_{\{u3,u4\}} - R_{\{u2,u3\}} - R_{\{u1,u4\}} - R_{\{u4,u8\}} - \quad (4.18)$$

$$-R_{\{u4,u9\}} - R_{\{u4,u10\}}$$

На рівні зв'язності q=5 ризик розраховується через уразливості, що залежать від загроз u_1, u_2, u_3, u_4, u_5, u_6, u_8, u_9, u_{10}, u_{13} з поправками на примикання примикання.

Розрахунок ризиків для цього рівня зв'язності здійснюється за формулами (4.19) – (4.27).

$$R_{u5} = \sum_{i=1}^{\{2,3,13,14,15\}} R_{b_i} + \sum_{i=1,i\neq j}^{\{2,3,13,14,15\}} R_{b_{\{i,j\}}} + \sum_{i=1,i\neq j\neq k}^{\{2,3,13,14,15\}} R_{b_{\{i,j,k\}}} + \cdots + R_{b_{\{1,2,3,13,14,15\}}} \quad (4.19)$$

$$R_{u13} = \sum_{i=1}^{\{6,8,10,11,12\}} R_{b_i} + \sum_{i=1,i\neq j}^{\{6,8,10,11,12\}} R_{b_{\{i,j\}}} + \sum_{i=1,i\neq j\neq k}^{\{6,8,10,11,12\}} R_{b_{\{i,j,k\}}} + \cdots + R_{b_{\{1,6,8,10,11,12\}}} \quad (4.20)$$

$$R_{\{u1,u3\}} = R_{b1,b5,b12,b13,b14,b15} \quad (4.21)$$

$$R_{\{u1,u6\}} = R_{b1,b5,b6,b13,b14,b15} \quad (4.22)$$

$$R_{\{u3,u5\}} = R_{\{u4,u5\}} = R_{\{u5,u6\}} = R_{b1,b2,b3,b13,b14,b15} \quad (4.23)$$

$$R_{\{u3,u8\}} = R_{\{u3,u9\}} = R_{b1,b2,b3,b9,b13,b14} \quad (4.24)$$

$$R_{\{u3,u10\}} = R_{b1,b2,b3,b9,b13} \quad (4.25)$$

$$R_{\{u4,u13\}} = R_{b1,b6,b8,b10,b11,b12} \quad (4.26)$$

$$R_{\{u8,u10\}} = R_{\{u9,u10\}} = R_{b1,b2,b3,b6,b9,b13} \quad (4.27)$$

Окремі склейки повторюються, тому їх не враховуємо.

Нижче наведено загальну формулу розрахунку ризику для цього рівня зв'язності (4.28).

$$\begin{aligned} R_{u1,u2,u3,u4,u5,u6,u8,u9,u10,u13} = \\ = R_{u1} + R_{u2} + R_{u3} + R_{u4} + R_{u5} + R_{u6} + R_{u8} + R_{u9} + \\ + R_{u10} + R_{u13} - R_{\{u6,u4\}} - R_{\{u3,u4\}} - R_{\{u2,u3\}} - \\ - R_{\{u1,u4\}} - R_{\{u4,u8\}} - R_{\{u4,u9\}} - R_{\{u4,u10\}} - \\ - R_{\{u4,u5\}} - R_{\{u4,u13\}} \end{aligned} \quad (4.28)$$

На рівні зв'язності q=4 ризик розраховується через уразливості, що залежать від загроз u1, u2, u3, u4, u5, u6, u7, u8, u9, u10, u13, з поправками на примикання.

Розрахунки ризиків для цього рівня зв'язності здійснюється за формулами (4.29) – (4.34).

$$R_{u7} = \sum_{i=1}^{\{2,3,7,13\}} R_{b_i} + \sum_{i=1,i\neq j}^{\{2,3,7,13\}} R_{b_{\{i,j\}}} + \sum_{i=1,i\neq j\neq k}^{\{2,3,7,13\}} R_{b_{\{i,j,k\}}} + \cdots + R_{b_{\{1,2,3,7,13\}}} \quad (4.29)$$

$$R_{\{u1,u2\}} = R_{b5,b12,b13,b14,b15} \quad (4.30)$$

$$R_{\{u3,u13\}} = R_{b1,b8,b10,b11,b12} \quad (4.31)$$

$$R_{\{u4,u7\}} = R_{b1,b2,b3,b7,b13} \quad (4.32)$$

$$R_{\{u5,u8\}} = R_{\{u5,u9\}} = R_{b1,b2,b3,b13,b14} \quad (4.33)$$

$$R_{\{u5,u10\}} = R_{b1,b2,b3,b13,b15} \quad (4.34)$$

$$R_{\{u6,u7\}} = R_{b1,b2,b3,b7,b13} \quad (4.34)$$

Оскільки окремі склейки були прораховані раніше, тому враховуємо тільки ті, що з'явилися на цьому рівні.

Загальний ризик для цього рівня зв'язності розраховується за формулою (4.35):

$$\begin{aligned} R_{u1,u2,u3,u4,u5,u6,u7,u8,u9,u10,u13} = = R_{u1} + R_{u2} + R_{u3} + R_{u4} + R_{u5} + R_{u6} + R_{u7} + R_{u8} + \\ + R_{u9} + R_{u10} + R_{u13} - R_{\{u6,u4\}} - R_{\{u3,u4\}} - R_{\{u2,u3\}} - \\ - R_{\{u1,u4\}} - R_{\{u4,u8\}} - R_{\{u4,u9\}} - R_{\{u4,u10\}} - R_{\{u4,u5\}} - \\ - R_{\{u4,u13\}} - R_{\{u4,u7\}} \end{aligned} \quad (4.35)$$

На рівні зв'язності q=3 ризик розраховується через уразливості, що залежать від загроз u1, u2, u3, u4, u5, u6, u7, u8, u9, u10, u11, u12, u13, u14, з поправками на примикання.

Розрахунки ризиків для цього рівня зв'язності здійснюється за формулами (4.36) – (4.46).

$$R_{u11} = \sum_{i=1}^{\{2,11,13\}} R_{b_i} + \sum_{i=1, i\neq j}^{\{2,11,13\}} R_{b_{\{i,j\}}} + \sum_{i=1, i\neq j\neq k}^{\{2,11,13\}} R_{b_{\{i,j,k\}}} + \cdots + R_{b_{\{1,2,11,13\}}} \quad (4.36)$$

$$R_{u12} = \sum_{i=1}^{\{6,8,12\}} R_{b_i} + \sum_{i=1, i\neq j}^{\{6,8,12\}} R_{b_{\{i,j\}}} + \sum_{i=1, i\neq j\neq k}^{\{6,8,12\}} R_{b_{\{i,j,k\}}} + \cdots + R_{b_{\{1,6,8,12\}}} \quad (4.37)$$

$$R_{u14} = \sum_{i=1}^{\{2,3,13\}} R_{b_i} + \sum_{i=1, i\neq j}^{\{2,3,13\}} R_{b_{\{i,j\}}} + \sum_{i=1, i\neq j\neq k}^{\{2,3,13\}} R_{b_{\{i,j,k\}}} + \cdots + R_{b_{\{1,2,3,13\}}} \quad (4.38)$$

$$R_{\{u1,u5\}} = R_{b1,b13,b14,b15} \quad (4.39)$$

$$R_{\{u1,u8\}} = R_{b1,b6,b14,b13} \quad (4.40)$$

$$R_{\{u1,u9\}} = R_{b1,b6,b13,b14} \quad (4.41)$$

$$R_{\{u1,u10\}} = R_{b1,b6,b14,b15} \quad (4.42)$$

$$R_{\{u3,u7\}} = R_{\{u3,u14\}} = R_{\{u4,u14\}} = R_{\{u5,u14\}} = R_{\{u6,u14\}} = R_{\{u7,u14\}} == R_{\{u7,u10\}} = R_{\{u7,u8\}} = R_{\{u7,u9\}} = R_{\{u8,u14\}} == R_{\{u9,u14\}} = R_{\{u10,u14\}} = R_{\{u12,u13\}} = R_{b1,b13,b2,b3} \quad (4.43)$$

$$R_{\{u3,u11\}} = R_{\{u4,u11\}} = R_{\{u5,u7\}} = R_{b1,b13,b2,b11} \quad (4.44)$$

$$R_{\{u4,u12\}} = R_{b1,b6,b8,b12} \quad (4.45)$$

$$R_{\{u6,u13\}} = R_{b1,b6,b8,b10} \quad (4.46)$$

Загальний ризик для цього рівня зв'язності розраховується за формулою (4.47).

$$R_{u1,u2,u3,u4,u5,u6,u7,u8,u9,u10,u11,u12,u13,u14} = R_{u1} + \\ + R_{u2} + R_{u3} + R_{u4} + R_{u5} + R_{u6} + R_{u7} + R_{u8} + R_{u9} + R_{u10} + \\ + R_{u11} + R_{u12} + R_{u13} + R_{u14} - R_{\{u6,u4\}} - R_{\{u3,u4\}} - \\ - R_{\{u2,u3\}} - R_{\{u1,u4\}} - R_{\{u4,u8\}} - R_{\{u4,u9\}} - R_{\{u4,u10\}} - \\ - R_{\{u4,u5\}} - R_{\{u4,u13\}} - R_{\{u4,u7\}} - R_{\{u3,u11\}} - R_{\{u4,u12\}} - R_{\{u3,u14\}} \quad (4.47)$$

На рівні зв'язності q=2 загальний ризик не змінюється, але з'являються додаткові зв'язки, які вже враховані на попередніх етапах.

Розрахунки ризиків для цього рівня зв'язності здійснюється за формулами (4.48) – (4.55).

$$R_{\{u1,u13\}} = R_{b1,b12} \quad (4.48)$$

$$R_{\{u1,u12\}} = R_{b1,b6,b12} \quad (4.49)$$

$$R_{\{u2,u5\}} = R_{b15,b13,b14} \quad (4.50)$$

$$R_{\{u2,u8\}} = R_{\{u2,u9\}} = R_{b9,b13,b14} \quad (4.51)$$

$$R_{\{u2,u10\}} = R_{b9,b13,b15} \tag{4.52}$$

$$R_{\{u3,u12\}} = R_{b1,b8,b12} \tag{4.53}$$

$$R_{\{u5,u11\}} = R_{\{u6,u11\}} = R_{\{u7,u11\}} = R_{\{u8,u11\}} = R_{\{u9,u11\}} == R_{\{u10,u11\}} = R_{b1,b2,b13} \tag{4.54}$$

$$R_{\{u6,u12\}} = R_{b1,b6,b8} \tag{4.55}$$

Загальний ризик для цього рівня зв'язності розраховується за формулою (4.56).

$$\begin{gathered} R_{u1,u2,u3,u4,u5,u6,u7,u8,u9,u10,u11,u12,u13,u14} = R_{u1} + R_{u2} + R_{u3} + \\ + R_{u4} + R_{u5} + R_{u6} + R_{u7} + R_{u8} + R_{u9} + R_{u10} + R_{u11} + R_{u12} + \\ + R_{u13} + R_{u14} - R_{\{u6,u4\}} - R_{\{u3,u4\}} - R_{\{u2,u3\}} - R_{\{u1,u4\}} - \\ - R_{\{u4,u8\}} - R_{\{u4,u9\}} - R_{\{u4,u10\}} - R_{\{u4,u5\}} - R_{\{u4,u13\}} - \\ - R_{\{u4,u7\}} - R_{\{u3,u11\}} - R_{\{u4,u12\}} - R_{\{u3,u14\}} \end{gathered} \tag{4.56}$$

На рівні зв'язності q=1 загальний ризик через загрози не змінюється тому, що нових уразливостей на цьому рівні не виникає. З'являються додаткові зв'язки, які також прораховуються.

Ризики для цього рівня зв'язності розраховується за формулами (4.57) – (4.61).

$$R_{\{u1,u7\}} = R_{\{u1,u11\}} = R_{\{u1,u14\}} = R_{b1,b13} \tag{4.57}$$

$$R_{\{u2,u11\}} = R_{b11,b13} \tag{4.58}$$

$$R_{\{u2,u12\}} = R_{b8,b12} \tag{4.59}$$

$$R_{\{u8,u12\}} = R_{\{u9,u12\}} = R_{\{u9,u13\}} = R_{\{u10,u12\}} = R_{\{u10,u13\}} = R_{b1,b6} \tag{4.60}$$

$$R_{\{u11,u13\}} = R_{b1,b11} \tag{4.61}$$

Загальний ризик для цього рівня зв’язності розраховується за формулою (4.62).

$$R_{u1,u2,u3,u4,u5,u6,u7,u8,u9,u10,u11,u12,u13,u14} = R_{u1} + R_{u2} + \\ +R_{u3} + R_{u4} + R_{u5} + R_{u6} + R_{u7} + R_{u8} + R_{u9} + R_{u10} + R_{u11} + \\ +R_{u12} + R_{u13} + R_{u14} - R_{\{u6,u4\}} - R_{\{u3,u4\}} - R_{\{u2,u3\}} - R_{\{u1,u4\}} - \\ -R_{\{u4,u8\}} - R_{\{u4,u9\}} - R_{\{u4,u10\}} - R_{\{u4,u5\}} - R_{\{u4,u13\}} - R_{\{u4,u7\}} - \\ -R_{\{u3,u11\}} - R_{\{u4,u12\}} - R_{\{u3,u14\}} \quad (4.62)$$

На рівні зв’язності q=0 загальний ризик через загрози не змінюється тому, що нових уразливостей на цьому рівні не виникає. З’являються додаткові зв’язки, які також прораховуються.

Ризики для цього рівня зв’язності розраховується за формулами (4.63) – (4.64).

$$R_{\{u2,u7\}} = R_{\{u2,u14\}} = R_{b13} \quad (4.63)$$

$$R_{\{u5,u12\}} = R_{\{u5,u13\}} = R_{\{u7,u12\}} = R_{\{u7,u13\}} = R_{\{u11,u12\}} = R_{\{u12,u14\}} = R_{\{u13,u14\}} = R_{b1} \quad (4.64)$$

Загальний ризик для цього рівня зв’язності розраховується за формулою (4.65).

$$R_{u1,u2,u3,u4,u5,u6,u7,u8,u9,u10,u11,u12,u13,u14} = R_{u1} + R_{u2} + \\ +R_{u3} + R_{u4} + R_{u5} + R_{u6} + R_{u7} + R_{u8} + R_{u9} + R_{u10} + R_{u11} + R_{u12} + \\ +R_{u13} + R_{u14} - R_{\{u6,u4\}} - R_{\{u3,u4\}} - R_{\{u2,u3\}} - R_{\{u1,u4\}} - R_{\{u4,u8\}} - \\ -R_{\{u4,u9\}} - R_{\{u4,u10\}} - R_{\{u4,u5\}} - R_{\{u4,u13\}} - R_{\{u4,u7\}} - R_{\{u3,u11\}} - \\ -R_{\{u4,u12\}} - R_{\{u3,u14\}} \quad (4.65)$$

Важливим етапом є прорахунок втрат для кожної загрози через потенційні втрати від уразливостей. У загальному випадку, коли відомі рівні

втрат від конкретної загрози та їх потенційні сумісні реалізації, то для їх розрахунку можна використовувати формулу (4.65).

В умовах підвищення рівня ризику для ІСОКІ, зокрема через поширення фішингових атак, ботнетів, застосування зараженого вірусами програмного забезпечення, «програм-вимагачів» тощо [109], специфічним підходом є виявлення вразливостей інформаційних ресурсів (далі – ІР) ІСОКІ. Для визначення ризику можливих кібератак пропонується застосувати розрахункові методи оцінювання потенційних загроз.

Для обрахування втрат від реалізації загроз (кібератак) необхідні значення коефіцієнтів деструкції вразливих компонентів ІР ІСОКІ. Їх значення мають відповідати затратам на відновлення штатного стану відповідних компонентів та можуть бути точно оцінені по кошторисах відповідних відновлюваних робіт. Звісно, зовнішній (системний) ефект деструкції може значно перевищувати суму цих затрат, тому його оцінка має проводитися окремо на основі експертних висновків.

У рамках цього дослідження для демонстраційного прикладу розрахунку втрат і ризиків від кібератак обмежимось грубими оцінками, використовуючи категоріальну шкалу, наведену в таблиця 4.3.

Для проведення подальших розрахунків ризику фактично застосовується лише оцінка сумарних втрат, наведена в останньому рядку таблиці 4.3.

При цьому, сама таблиця 4.3 відображає один із способів оцінювання втрат, породжених реалізацією відповідної вразливості внаслідок проведеної кібератаки.

Таблиця 4.3 – Категоріальні оцінки деструкції від вразливостей КІ

	Уразливості														
Деструкції	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9	b_{10}	b_{11}	b_{12}	b_{13}	b_{14}	b_{15}
Софт	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0
Хард	0	0	0	0	0	0	0	1	0	1	1	0	0	0	1
Дані	0	0	0	0	1	0	0	0	1	1	1	1	1	0	0
Зовнішній ефект	1	1	1	1	2	2	3	3	3	3	3	4	4	1	1
Сумарні втрати	**2**	**2**	**2**	**2**	**4**	**3**	**4**	**5**	**5**	**6**	**6**	**6**	**6**	**2**	**2**

Для прорахунку ризиків, окрім втрат, маємо визначити їх ймовірність. Але ймовірнісний розподіл сумісної реалізації вразливостей залежить від характеристик реальних атак. У реальних інцидентах оцінки ризику за фактом реалізації загроз можуть відрізнятися. У випадку, коли існує статистичний розподіл виникнення тих чи інших втрат від реалізації загроз, що зокрема, залежать від наявності в системі переліку вразливостей, які сумісно впливають на їх виникнення, можна використовувати частоту виникнення загроз для оцінки ймовірності вразливостей, а також застосовувати такі показники як рівень впливовості окремих загроз. У таблиці 4.4 наведено показники (розрахунки) загального рівня втрат у залежності від окремих визначених загроз.

Таблиця 4.4 - Рівень втрат для кожної загрози в системі

	u_1	u_2	u_3	u_4	u_5	u_6	u_7	u_8	u_9	u_{10}	u_{11}	u_{12}	u_{13}	u_{14}	**Σ**
Загальний рівень втрат (V_i)	25	42	48	55	16	43	16	22	22	22	16	16	28	12	**383**

У таблиці 4.5 наведено показники (розрахунки) втрат від склейки для кожної склейки симплексів загроз в системі.

Таблиця 4.5 - Рівень втрат для кожної склейки симплексів загроз в системі

Склейка	**Втрати від склейки**
$V_{\{u3,u4\}}$	48
$V_{\{u2,u3\}}$	42
$V_{\{u1,u4\}}$	25
$V_{\{u4,u8\}}$	22
$V_{\{u4,u9\}}$	22
$V_{\{u4,u10\}}$	22
$V_{\{u4,u5\}}$	16
$V_{\{u4,u13\}}$	28
$V_{\{u4,u7\}}$	16
$V_{\{u3,u11\}}$	16
$V_{\{u4,u12\}}$	16
$V_{\{u3,u14\}}$	12
$V_{\{u6,u4\}}$	43
Σ	328

Після проведених обчислень здійснюється оцінка загроз та ризиків, ймовірність практичної реалізації яких є найвищою. Для проведення розрахунку ризиків припускається, що сумісна реалізація несприятливих подій, зокрема від кібератаки, є незалежною за втратами. Тому ризики розраховуються як сума, а ймовірність події як – добуток.

Загальний ризик розраховується за формулою (4.66).

$$\begin{gathered} R_{u1,u2,u3,u4,u5,u6,u7,u8,u9,u10,u11,u12,u13,u14} = p_{u_1}V_{u1} + p_{u_2}V_{u2} + +p_{u_3}V_{u3} + \\ p_{u_4}V_{u4} + p_{u_5}V_{u5} + \\ +p_{u_6}V_{u6} + p_{u_7}V_{u7} + p_{u_8}V_{u8} + p_{u_9}V_{u9} + p_{u_{10}}V_{u10} + p_{u_{11}}V_{u11} + \\ +p_{u_{12}}V_{u12} + p_{u_{13}}V_{u13} + p_{u_{14}}V_{u14} - p_{u_6}p_{u_4}V_{\{u6,u4\}} - p_{u_3}p_{u_4}V_{\{u3,u4\}} - \\ -p_{u_2}p_{u_3}V_{\{u2,u3\}} - p_{u_1}p_{u_4}V_{\{u1,u4\}} - p_{u_4}p_{u_8}V_{\{u4,u8\}} - p_{u_4}p_{u_9}V_{\{u4,u9\}} - \\ -p_{u_4}p_{u_{10}}V_{\{u4,u10\}} - p_{u_4}p_{u_5}V_{\{u4,u5\}} - p_{u_4}p_{u_{13}}V_{\{u4,u13\}} - \\ -p_{u_4}p_{u_7}V_{\{u4,u7\}} - p_{u_3}p_{u_{11}}V_{\{u3,u11\}} - p_{u_4}p_{u_{12}}V_{\{u4,u12\}} - p_{u_3}p_{u_{14}}V_{\{u3,u14\}} \end{gathered} \tag{4.66}$$

Оскільки для досліджуваної ІСОКІ вже були розраховані показники (розрахунки) втрат для кожної загрози в системі та для кожної склейки

симплексів загроз в системі, то відповідні величини наведені в таблицях 4.4 та 4.5.

З урахуванням зазначених вище показників загальний ризик для досліджуваної ІСОКІ розраховується за формулою (4.67) і залежить лише від ймовірності реалізації подій.

$$\begin{aligned} R_{u1,u2,u3,u4,u5,u6,u7,u8,u9,u10,u11,u12,u13,u14} = \\ = 25p_{u_1} + 42p_{u_2} + 48p_{u_3} + 55p_{u_4} + 16p_{u_5} + 43p_{u_6} + \\ +16p_{u_7} + 22p_{u_8} + 22p_{u_9} + 22p_{u_{10}} + 16p_{u_{11}} + 16p_{u_{12}} + 28p_{u_{13}} + \\ +12p_{u_{14}} - 43p_{u_6}p_{u_4} - 48p_{u_3}p_{u_4} - 42p_{u_2}p_{u_3} - 25p_{u_1}p_{u_4} - \\ -22p_{u_4}p_{u_8} - 22p_{u_4}p_{u_9} - 22p_{u_4}p_{u_{10}} - 16p_{u_4}p_{u_5} - 28p_{u_4}p_{u_{13}} - \\ -16p_{u_4}p_{u_7} - 16p_{u_3}p_{u_{11}} - 16p_{u_4}p_{u_{12}} - 12p_{u_3}p_{u_{14}} \end{aligned} \quad (4.67)$$

Наведена формула 4.67 свідчить про те, що залежність загального ризику від ймовірності реалізації подій для досліджуваної ІСОКІ описується квадратичною функцією, яку можна дослідити аналітично, для виявлення екстремумів та характерних точок.

Окрім цього, накладаються додаткові умови на визначення ймовірностей p_{u_i} (формули (4.68) – (4.69)).

$$p_{u_i} \in [0; 1]; \quad (4.68)$$

$$U = \sum_{i=1}^{14} p_{u_i} = 1 \quad (4.69)$$

Функція, які описуються формулою (4.66), а з урахуванням умов, які описуються формулами (4.68) – (4.69), відноситься до задач лінійного програмування (оптимізації), які можна розв’язати за допомогою методу Лагранжа.

Формулами (4.70) – (4.71) описується функція Лагранжа та похідні за всіма параметрами.

$$L = R_{u1,u2,u3,u4,u5,u6,u7,u8,u9,u10,u11,u12,u13,u14} - \lambda U; \quad (4.70)$$

$$\begin{cases} \frac{\partial L}{\partial p_{u_i}} = 0 \\ \frac{\partial L}{\partial \lambda} = 0 \end{cases} \quad (4.71)$$

За результатом проведених розрахунків за формулами (4.7) та (4.71), отримуємо, що $\lambda = 0$, всі $p_{u_i} = 0$, окрім $p_{u_3} = 1$ та $p_{u_4} = 1$. Очевидно, що одночасно дорівнювати одиниці вони не можуть тому, що не виконується обмеження (4.69). Якщо підставляти значення ймовірностей окремо, то отримуємо при $p_{u_3} = 1$ величина ризику $R = 48$, а при $p_{u_4} = 1$ відповідно $R = 55$. Очевидно, що роподіл при якому тільки $p_{u_4} = 1$ буде точкою максимума при оцінці ризику. Це є логічним, оскільки ця компонента відповідає найбільшому рівню втрат, а при інших розподілах виникає від'ємна частина (ймовірність), яка зменшує при оцінці загальну величину ризику.

З іншої точки зору, необхідно також визначити умови, при яких значення ризику буде мінімальним. Оскільки розрахунки, проведені за допомогою метода Лагранжа, не надають однозначної відповіді на це питання, то пошук мінімальних значень ризику необхідно здійснювати в крайніх точках значень розподілу ймовірності загроз, тобто почергово занулюючи всі p_{u_i} крім одного.

За допомогою методу Лагранжа було розраховано, що максимальними значення ризику стають при подіях *i=3* та *i=4*. Шляхом перебору крайніх точок отримуємо результат, за яким мінімальним значення ризику буде при реалізації події *i=14*. У інших випадках величина ризику буде зростати швидше за від'ємну частину (ймовірність), щоб нівелювати зростання основного ризику.

На рисунку 4.11 наведено графік величини оцінки ризику в залежності від можливих розподілів ймовірності загроз, відповідно до профілів атак. Унаслідок багатокомпонентності вектору ймовірностей, що використовується

як вхід до функції оцінки ризику, застосуємо як область визначення – відрізок між двома точками. Він задається як опукла лінійна комбінація векторів кінців з коефіцієнтами α та (1-α), де 0 ≤ α ≤ 1. Заміняємо $R(p_{u_i})$, що залежить від вектора ймовірностей, на $R\left(p_{u_i}(\alpha)\right)$, що залежить від одного параметра α, для можливості відобразити багатовимірний простір на площині. У формулі (4.72) наведено перетворення багатокомпонентного вектора у однопараметричну форму.

$$p_{u_i}(\alpha) = \alpha \cdot p^1_{u_\text{i}} + (1-\alpha) \cdot p^2_{u_\text{i}} \qquad (4.72)$$

де $p^1_{u_\text{i}}$ – значення вектора ймовірностей, що відповідає мінімуму функції ризику;

$p^2_{u_\text{i}}$ – значення вектора ймовірностей, що відповідає мінімуму функції ризику.

Графік має узагальнений вигляд. Точки екстремуму представляють найбільший інтерес для аналізу отриманої формули (4.67), тому вони були обрані в якості векторів кінців відрізку. Відповідно максимальний та мінімальний ризик відображено крайніми точками графіку. Графік стандартної оцінки ризику відповідає лінійній залежності від розподілу ймовірностей без врахування структури зв’язків між загрозами. Графік уточненої оцінки відповідає поліноміальної формулі ризику, що враховує взаємозалежності та сумісності реалізацій загроз та ймовірнісного розподілу у профілі атак.

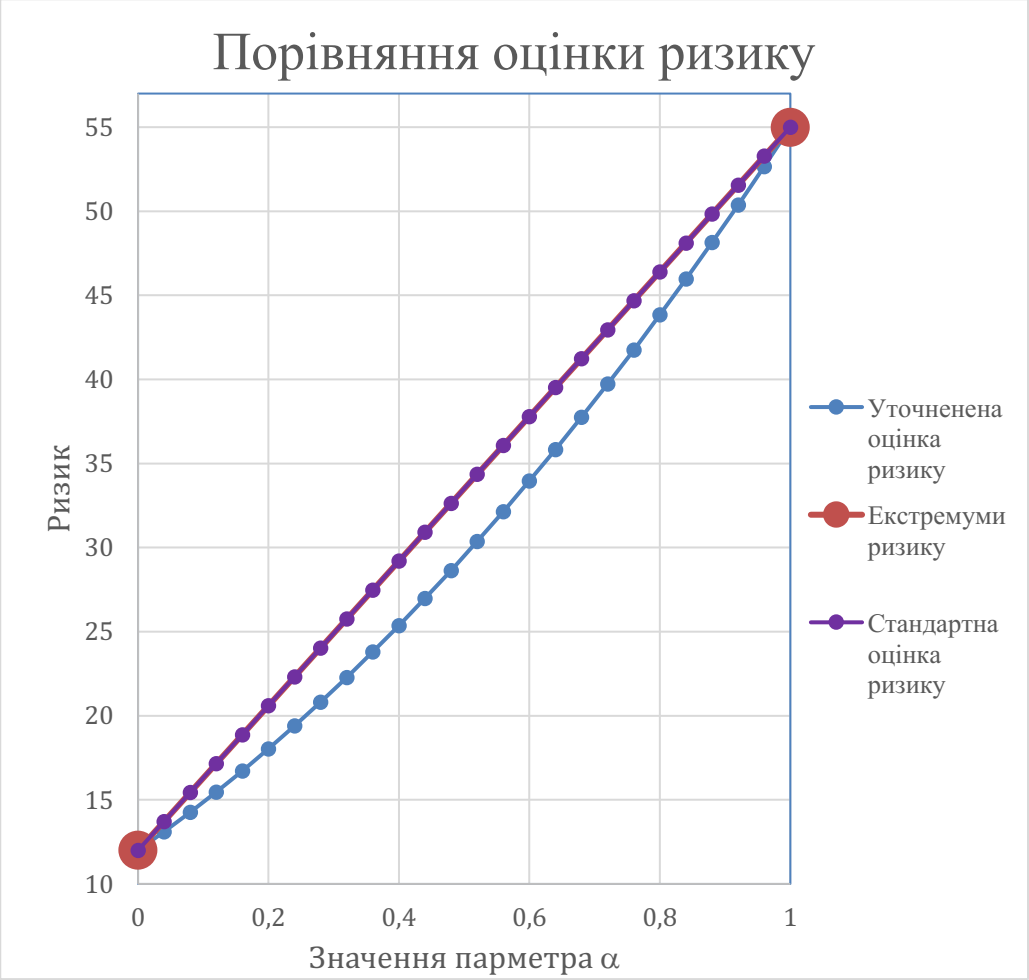


Рисунок 4.11 – Порівняння значень оцінки ризику

Припустимо, що розподіл виникнення загроз є рівномірним. У такому випадку, ймовірності розраховуються за формулами (4.73) – (4.74).

$$p_{u_i} = \frac{1}{14} \tag{4.73}$$

$$p_{\{u_i u_j\}} = \frac{1}{14} \cdot \frac{1}{14} \tag{4.74}$$

Розрахунок загального ризику, проведеного у рамках запропонованого методу, здійснюється за формулою (4.75).

$$\begin{aligned} R_{\text{уточнена}(u1,u2,u3,u4,u5,u6,u7,u8,u9,u10,u11,u12,u13,u14)} \\ = \frac{1}{14}\sum_{1}^{14} V_{ui} - \\ - \frac{1}{14^2}\left(V_{\{u6,u4\}} + V_{\{u3,u4\}} + V_{\{u2,u3\}} + V_{\{u1,u4\}} + V_{\{u4,u8\}} + V_{\{u4,u9\}}\right. \\ + V_{\{u4,u10\}} + V_{\{u4,u5\}} + V_{\{u4,u13\}} + V_{\{u4,u7\}} + V_{\{u3,u11\}} + V_{\{u4,u12\}} \\ \left. + V_{\{u3,u14\}}\right) = \frac{383}{14} - \frac{328}{196} = \frac{5034}{196} \approx 25{,}68 \end{aligned} \tag{4.75}$$

Загальний ризик без урахування структури зв’язків у системі розраховується за формулою (4.76).

$$R_{\text{стандартна}(u1,u2,u3,u4,u5,u6,u7,u8,u9,u10,u11,u12,u13,u14)} = \\ = \sum_{1}^{14} R_{ui} = \frac{1}{14}\sum_{1}^{14} V_{ui} = \frac{383}{14} = 27.36 \tag{4.76}$$

Результати розрахунків, отримані за формулами (4.75) та (4.76), дозволяють здійснити порівняльний аналіз величин ризиків, розрахованих за допомогою узагальненого методу оцінки ризику, та за спрощеною процедурою лінійної оцінки, та оцінити рівень уточнення ризику за формулою (4.77).

$$\varepsilon_R = \frac{R_c - R_y}{R_c} \cdot 100\% \approx \frac{27.36 - 25.68}{27.36} \cdot 100\% \approx 6.1\% \tag{4.77}$$

Отриманий результат свідчить про те, що практичне застосування запропонованого методу оцінювання ризику у порівнянні із спрощеною лінійною оцінкою дозволило знизити загальний ризик для досліджуваної інформаційної системи об’єкта критичної інфраструктури приблизно на 6,1%.

Додатковим уточненням є те, що при розрахунках доданки, пов’язані з окремими ризиками R_i, скорочуються з відніманням на склейки, оскільки, ураховуючи структури деяких загроз u_i, вони є частиною загрози u_j, тобто не несуть додаткової інформації для оцінки ризику, адже вони вже враховані у ризиках R_i.

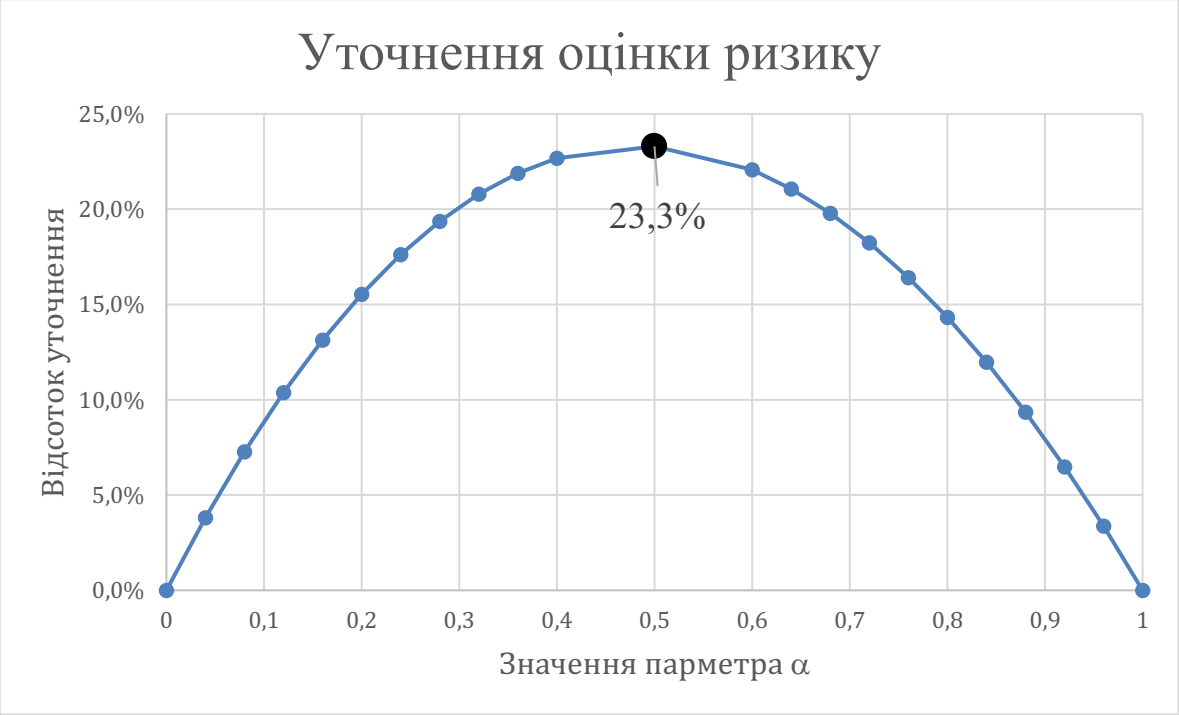


Рисунок 4.12 – Уточнення відносної поправки в оцінці ризику в залежності від ймовірнісного розподілу виникнення загроз

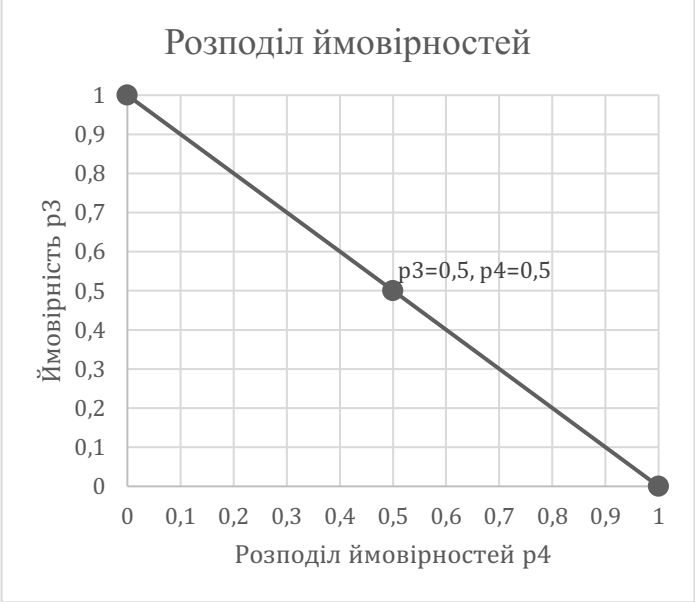


Рисунок 4.13 – Відрізок між ймовірностями, при яких відбувається зміна максимального відносного уточнення стандартної оцінки ризику

На рисунку 4.12 наведено графік функції, якими описується залежність величини відносної поправки на «склейки» у формулі оцінки ризику від параметра α, який як і у випадку порівняння оцінки ризику введенений для розрахунку зведення багатокомпонентного вектора розподілу ймовірностей до

однопараметричного задання на відрізку, кінцями якого є розподіл ймовірності виникнення загроз для певного профілю атак. Графік свідчить про те, що величина відносної поправки змінюється від нуля (в даному випадку $\alpha = 0$, при розподілах ймовірностей $p_3 = 1$ та $p_i = 0$), далі зростає до максимального рівня ε_R=23,3% при $\alpha = 0{,}5$ і зменшується до нуля. При $\alpha = 1$ величина відносної поправки відповідає розподілу ймовірностей $p_3 = 0$ та $p_i = 1$. Унаслідок виродження чотирнацятимірного розподілу до двомірного є можливість зобразити відрізок переходу з одного мінімального значення поправки до іншого. Відповідні розподіли ймовірностей наведені на рисунку 4.13 та відповідають крайнім точкам. Точки $p_3 = 0{,}5$ та $p_4 = 0{,}5$ відповідають максимуму функції на рисунку 4.12.

Отриманий результат підтверджує універсальність, ефективність та практичну значимість запропонованого методу оцінювання ризику, і дозволяє надати додаткові рекомендації щодо формування вимог до вхідних даних. У випадку, коли окремі симплекси є частинами іншого симплексу (загрози вкладені в інші загрози), їх можна ігнорувати при оцінці ризику. Первині перевірки вкладення можна провести вже на етапі формування матриці інцидентності.

Висновки до розділу 4

У розділі представлено застосування розробленого методу розрахунку оцінки та аналізу ризиків від загроз та вразливостей для інформаційної системи об’єкта критичної інфраструктури. Наведено основні етапи процедури виявлення та аналізу сумісності вразливостей між собою та систему загроз в цілому.

Розглянуто та застосовано алгоритм побудови симплеціального комплексу та структурного дерева з подальшим аналізом взаємозв’язку між уразливостями на прикладі інформаційної системи об’єкта критичної інфраструктури.

Доведено, що деякі вразливості, які часто не виявляються при зборі даних про систему, можуть мати значний, хоча і непрямий вплив на надійність, доступність та цілісність системи в цілому.

Здійснено структурну класифікацію наявних загроз в інформаційній системі об’єкта критичної інфраструктури на основі Q-аналізу.

На основі проведеного аналізу було виконано оцінювання ризику для наведеної інформаційної системи об’єкта критичної інфраструктури та проведено застосування відповідного методу на реальних даних. Здійснено побудову формули байєсової оцінки ризику з урахуванням впливу дослідженої складної структури системи загроз.

Застосування запропонованого методу оцінювання ризику для дослідженого практичного прикладу показало, що у порівнянні із спрощеною лінійною оцінкою загальний ризик для інформаційної системи об’єкта критичної інфраструктури знижується на 0÷23,3% в залежності від розподілу загроз та профілю атак.

ВИСНОВКИ

Дисертаційну роботу присвячено розв’язанню актуальної наукової задачі аналізу та синтезу моделей і методів оцінювання ризиків з врахуванням структурних властивостей сукупності зв’язків загроз та вразливостей кіберсистем, що дозволяє розробити процедуру побудови формули байєсівської оцінки ризику, виконати її аналіз та забезпечити уточнення оцінки ризику внаслідок врахування структури сумісності вразливостей системи.

За результатами проведеного дослідження у рамках цієї дисертаційної роботи було отримано результати:

- Вперше побудовано модель зв’язків загроз та вразливостей у кіберсистемі у вигляді симплеціального комплексу, яка представляє складну структуру їх взаємозалежностей, для класифікації загроз і вразливостей та для оцінювання потенційних втрат і ризиків;
- Вперше розроблено алгоритми аналізу симплекційного комплексу та його синтезу на основі повного набору структурних характеристик комплексу;
- Вперше розроблено метод класифікації загроз та вразливостей у складній системі з урахуванням характеристик власної розмірності підсистем, їх примикання та наслідування, що дозволяє надійніше оцінювати ризики в кіберсистемі в залежності від варіантів атак;
- Розроблено процедуру побудови байєсівської оцінки ризику з врахуванням структури вразливостей системи та складеної функції втрат.

Доведено, що оцінка ризику, побудована за допомогою методу розрахунку ризиків у складній системі з урахуванням структури зв’язків загроз та вразливостей дозволяє отримати більш точні результати у порівнянні з байєсовою оцінкою ризику за спрощеною лінійною формулою. Для розглянутого прикладу оцінки ризику для вибраної системи критичної інфраструктури величина уточнення становить 0÷23,3% у залежності від ймовірнісного розподілу загроз та профілю атак.

Наукові напрацювання та пропозиції використані під час підготовки матеріалів до засідання Ради національної безпеки і оборони України з питання «Про стан справ у енергетичній сфері», рішення Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони, а також у процесі розроблення Загальних правил обміну інформацією про кіберінциденти, затверджених рішенням НКЦК.

Результати дослідження впроваджено у навчальний процес навчально-наукового фізико-технічного інституту НТУУ «КПІ імені Ігоря Сікорського». На основі результатів дослідження розроблено матеріали для лекційних та практичних занять для магістерських та аспірантських освітні програм підготовки за спеціальністю 125 «Кібербезпека та захист інформації».

Моделі та методи розроблені в дисертації використані в Науково-дослідні роботі «Підтримка прийняття рішень в умовах невизначеності та конкурентної взаємодії» номер державної реєстрації 0124U001957.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Полуциганова В. І., Смирнов С. А. Методологія побудови основних метрик q-аналізу та їх застосування. *Системні дослідження та інформаційні технології*. 2019. № 3. С. 76 – 88. URL: https://doi.org/10.20535/srit.2308-8893.2019.3.07 (date of access: 10.11.2023).

2. Polutsyganova V., Smirnov S. The inverse problem of Q-analysis of complex systems structure in cyber security. *Theoretical and applied cybersecurity*. 2023. Vol. 4, no. 1. URL: https://doi.org/10.20535/tacs.2664-29132022.1.274123 (date of access: 10.11.2023).

3. Polutsyhanova V. I. System construction of cybersecurity vulnerabilities with Q-analysis. *Theoretical and applied cybersecurity*. 2023. Vol. 5, no. 1. URL: https://doi.org/10.20535/tacs.2664-29132023.1.285430 (date of access: 08.11.2023).

4. Polutsyhanova V. I. Vulnerability classification using Q-analysis. *Theoretical and applied cybersecurity*. 2023. Vol. 5, no. 2. P. 56 – 61. URL: https://doi.org/10.20535/tacs.2664-29132023.2.285431 (date of access: 08.11.2023).

5. Медведенко В. І., Смирнов С. А. Використання q-аналізу для дослідження зв'язків у банківських системах. *XV Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики»*: Всеукр. науково-практ. конференція студентів, аспірантів та молодих вчен., м. Київ, 25 – 27 трав. 2017 р. Київ, 2017. С. 44 – 46.

6. Медведенко В. І., Смирнов С. А. Використання алгоритмів q-аналізу на прикладі банківської системи. *XVI Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики»*: Всеукр. науково-практ. конференція студентів, аспірантів та молодих вчен., м. Київ, 26 – 27 квіт. 2018 р. Київ, 2018. С. 33 – 36.

7. Polutsyhanova V. The inverse problem of q-analysis. *XVIII Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики»:* Всеукр. науково-практ. конференція студентів, аспірантів та молодих вчен., м. Київ, 12 – 13 трав. 2020 р. С. 113 – 115.

8. Полуциганова В. І., Смирнов С. А. The inverse problem of Q-analysis of comple x systems structure. *Інформаційні технології та безпека матеріали XXII міжнародної науково-практичної конференції випуск*, м. Київ, 2021. С. 114–118.

9. Полуциганова В. І., Смирнов С. А. Оцінювання ризиків складних систем з використання методів Q-аналізу. *Інформаційні технології та безпека матеріали XXIII міжнародної науково-практичної конференції випуск*, м. Київ, 2022. С. 51 – 52.

10. Полуциганова В. І., Смирнов С. А. Structure of vulnerability in complex systems and risk assessment// МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ «Виклики і загрози для критичної інфраструктури» 21 – 22 березня 2023 р. м. Київ, Україна. С. 334–335.

11. Полуциганова В. І., Смирнов С. А. Оцінка ризиків в кібербезпеці за допомогою Q-аналізу. *XXI Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики»*: Всеукр. науково-практ. конференція студентів, аспірантів та молодих вчен., м. Київ, 12 – 13 трав. 2023 р. Київ, 2017. С. 172 – 173.

12. Polutsyhanova V. I., Smirnov S. A. Assessing cybersecurity risk with Q-analysis. *Всеукраїнська науково-практична конференція «Theoretical and Applied Cybersecurity» (TACS-2023)*, Kyiv, 26 May 2023. P. 57 – 60.

13. Atkin R. Combinatorial connectivities in social systems: An application of simplicial complex structures to the study of large organizations. Basel : Birkhäuser, 1977. – 239 p.

14. Берёза О. А. Симплициальный анализ когнитивных карт социально-экономических систем. Известия Южного федерального университета. Технические науки, vol. 124, no. 11, 2011, pp. 151 – 161.

15. Beaumont J.R., Gatrell A.C. An introduction to Q-analysis Catmog 34, 1982. URL: https://alexsingleton.files.wordpress.com/2014/09/34-an-introduction-to-q-analysis.pdf.

16. Качинський А. Б. Безпека складних систем: математичне моделювання небезпечних процесів і системний аналіз її забезпечення. Київ: «Азимут-Україна», 2016. – 498 с.

17. Maletic S. V. Simplicial complexes and complex networks: the influence of higher-order (sub)structures on network properties [Текст]: дис. докт. / Maletic Slobodan V. – Beograd, 2013. – 65 с.

18. Avdeeva Z., Kovriga S. Cognitive Approach in Simulation and Plenary papers, Milestone reports & Selected survey papers. 17th IFAC World Congress, Seoul, Korea, July 2008. P. 160–167.

19. Gould P. Q-analysis, or a language of structure: an introduction for social scientists, geographers and planners. International journal of man-machine studies. 1980. Vol. 13, no. 2. P. 169–199. URL: https://doi.org/10.1016/s0020-7373(80)80009-5 (date of access: 03.12.2023).

20. Jeffrey H. J. “Some structures and notation of Q-analysis”, Environment and Planning B Planning and Design, (1981). doi: 10.1068/b080073.

21. Pierre Mazzega, Claire Lajaunie and Etienne Fieux “Governance Modeling: Dimensionality and Conjugacy”, Graph Theory - Advanced Algorithms and Applications, 2018. doi: 10.5772/intechopen.71774.

22. Duckstein, L. and Nobe, S. A. “Q-analysis for modeling and decision making”, European Journal of Operational Research, 103/3, (1997) 411–425. doi: 10.1016/S0377-2217(97)00308-1.

23. Maunder C. R. F. Algebraic topology. London, Van Nostrand Reinhold, 1970. – 375 p.

24. Atkin R. H. Mathematical structure in human affairs [Текст] / Atkin. – London: Heinemann Educational Books, 1973. – 143 с.

25. Atkin R. Mathematical structure in human affairs. London : Heinemann Educational, 1974. – 212 p.

26. Gould P., Gatrell A. A structural analysis of a game: The Liverpool v Manchester united cup final of 1977. Social networks. 1979. Vol. 2, no. 3. P. 253–273. URL: https://doi.org/10.1016/0378-8733(79)90017-0 (date of access: 03.12.2023).

27. Lake ecosystems: a polyhedral dynamics representation / J. Casti et al. Ecological modelling. 1979. Vol. 7, no. 3. P. 223–237. URL: https://doi.org/10.1016/0304-3800(79)90071-1 (date of access: 03.12.2023).

28. Johnson J. H. The Q-analysis of road traffic systems. Environment and planning B: planning and design. 1981. Vol. 8, no. 2. P. 141–189. URL: https://doi.org/10.1068/b080141 (date of access: 03.12.2023).

29. Johnson J., Wanmali S. A q-analysis of periodic market systems. Geographical analysis. 2010. Vol. 13, no. 3. P. 262–275. URL: https://doi.org/10.1111/j.1538-4632.1981.tb00734.x (date of access: 03.12.2023).

30. Sonis M., Hewings G. J. Introduction to input-output structural Q-analysis. 2000. – 43 p.

31. Bliemel M. J., McCarthy I. P., Maine E. M. A. An Integrated Approach to Studying Multiplexity in Entrepreneurial Networks. Entrepreneurship Research Journal. 2014. Vol. 4, no. 4. URL: https://doi.org/10.1515/erj-2014-0007 (date of access: 03.12.2023).

32. Maletić S., Zhao Y. Multilevel Integration Entropies: The Case of Reconstruction of Structural Quasi-Stability in Building Complex Datasets. Entropy. 2017. Vol. 19, no. 4. P. 172. URL: https://doi.org/10.3390/e19040172 (date of access: 03.12.2023).

33. Omer I., Goldblatt R. Using space syntax and Q-analysis for investigating movement patterns in buildings: The case of shopping malls. Environment and Planning B: Urban Analytics and City Science. 2016. Vol. 44, no.

3. P. 504–530. URL: https://doi.org/10.1177/0265813516647061 (date of access: 03.12.2023).

34. Gould P., Johnson J. National television policy. *Futures*. 1980. Vol. 12, no. 3. P. 178–190. URL: https://doi.org/10.1016/0016-3287(80)90021-x (date of access: 03.12.2023).

35. Gaspar, J.; Gould, P.. "The Cova da Beira: an applied structural analysis of agriculture and communication (Portugal). Lund Studies in Geography. 1981. Series B 48. P. 183-214. http://www.scopus.com/inward/record.url?eid=2-s2.0-0019703781&partnerID=MN8TOARS.

36. Johnson, J. H. Hypernetworks in the science of complex systems. Imperial College Press. 2014.

37. Johnson J. H. Q-transmission in simplicial complexes. International Journal of Man-Machine Studies. 1982. Vol. 16, no. 4. P. 351–377. URL: https://doi.org/10.1016/s0020-7373(82)80046-1 (date of access: 03.12.2023).

38. Casti J. L. Connectivity, complexity, and catastrophe in large-scale systems. Chichester [Eng.]: J. Wiley, 1979. – 203 p.

39. Parrish J. K. Complexity, pattern, and evolutionary trade-offs in animal aggregation. Science. 1999. Vol. 284, no. 5411. P. 99–101. URL: https://doi.org/10.1126/science.284.5411.99 (date of access: 04.12.2023).

40. Rind D. Complexity and Climate. Science. 1999. Vol. 284, no. 5411. P. 105–107. URL: https://doi.org/10.1126/science.284.5411.105 (date of access: 04.12.2023).

41. Wallace D. Everett and structure. Studies in History and Philosophy of Science Part B: Studies in History and Philosophy of Modern Physics. 2003. Vol. 34, no. 1. P. 87–105. URL: https://doi.org/10.1016/s1355-2198(02)00085-0 (date of access: 04.12.2023).

42. Weng G. Complexity in biological signaling systems. Science. 1999. Vol. 284, no. 5411. P. 92–96. URL: https://doi.org/10.1126/science.284.5411.92 (date of access: 04.12.2023).

43. Werner B. T. Complexity in natural landform patterns. Science. 1999. Vol. 284, no. 5411. P. 102–104. URL: https://doi.org/10.1126/science.284.5411.102 (date of access: 04.12.2023).

44. No man is an island. Nature Physics. 2009. Vol. 5, no. 1. P. 1. URL: https://doi.org/10.1038/nphys1162 (date of access: 04.12.2023).

45. Foote R. Mathematics and complex systems. Science. 2007. Vol. 318, no. 5849. P. 410–412. URL: https://doi.org/10.1126/science.1141754 (date of access: 04.12.2023).

46. Goldenfeld N. Simple lessons from complexity. Science. 1999. Vol. 284, no. 5411. P. 87–89. URL: https://doi.org/10.1126/science.284.5411.87 (date of access: 04.12.2023).

47. Arthur W. B. Complexity and the Economy. Science. 1999. Vol. 284, no. 5411. P. 107–109. URL: https://doi.org/10.1126/science.284.5411.107 (date of access: 04.12.2023).

48. Ladyman J., Lambert J., Wiesner K. What is a complex system?. *European Journal for Philosophy of Science*. 2012. Vol. 3, no. 1. P. 33–67. URL: https://doi.org/10.1007/s13194-012-0056-8 (date of access: 04.12.2023).

49. Mobus G. E., Kalton M. C. Principles of Systems Science. New York, NY: Springer New York, 2015. URL: https://doi.org/10.1007/978-1-4939-1920-8 (date of access: 09.09.2023).

50. Boccara N. Modeling Complex Systems. New York, NY: Springer New York, 2010. URL: https://doi.org/10.1007/978-1-4419-6562-2 (date of access: 09.09.2023).

51. Грицюк П. М., Джоші О. І., Гладка О. М. Основи теорії систем і управління: навч. посіб. Рівне: НУВГП, 2021. – 272 с.

52. Rausand M., Haugen S. Risk Assessment: Theory, Methods, and Applications. Wiley & Sons, Incorporated, John, 2020. – 784 p.

53. Diogenes Y., Ozkaya E. Cybersecurity – attack and defense strategies: infrastructure security with red team and blue team tactics. Packt Publishing, 2018. – 384 p.

54. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем: Навч.-метод. матеріали. Київ : Вид. група BHV, 2009. –698 с.

55. Новиков А. Н., Родионов А. Н., Тимошенко А. А. Модели и методы кибернетической защиты информационно-коммуникационных систем на основе логико-вероятностного подхода : монография. Киев : «Политехника», 2015. – 276 с.

56. Bacci S., Chiandotto B. Introduction to statistical decision theory. Chapman and Hall/CRC, 2019. URL: https://doi.org/10.1201/9781315112220 (date of access: 10.09.2023).

57. Le N. T., Hoang D. B. A Threat Computation Model using a Markov Chain and Common Vulnerability Scoring System and its Application to Cloud Security. Journal of Telecommunications and the Digital Economy. 2019. Vol. 7, no. 1. P. 37–56. URL: https://doi.org/10.18080/jtde.v7n1.181 (date of access: 28.07.2023).

58. Wald A. Statistical Decision Functions. The Annals of Mathematical Statistics. 1949. Vol. 20, no. 2. P. 165–205. URL: https://doi.org/10.1214/aoms/1177730030 (date of access: 06.12.2023).

59. Ferguson T. S. Mathematical statistics: A decision theoreticapproach. New York : Academic Press, 1967. – 396 p.

60. DeGroot M. H. Optimal statistical decisions. Wiley & Sons Ltd, 2004. –512 p.

61. JBerger J. O. Statistical Decision Theory and Bayesian Analysis. New York, NY : Springer New York, 1985. URL: https://doi.org/10.1007/978-1-4757-4286-2 (date of access: 06.12.2023

62. Piccinato L. Metodi per le decisioni statistiche. Milano : Springer Milan, 2009. URL: https://doi.org/10.1007/978-88-470-1106-9 (date of access: 06.12.2023).

63. Robert C. P., Chopin N., Rousseau J. Harold Jeffreys's Theory of Probability Revisited. Statistical Science. 2009. Vol. 24, no. 2. P. 141–172. URL: https://doi.org/10.1214/09-sts284 (date of access: 06.12.2023).

64. Defining and computing a value based cyber-security measure / A. B. Aissa et al. Information Systems and e-Business Management. 2011. Vol. 10, no. 4. P. 433–453. URL: https://doi.org/10.1007/s10257-011-0177-1 (date of access: 06.12.2023).

65. Identifying Attack Propagation Patterns in Honeypots Using Markov Chains Modeling and Complex Networks Analysis / A. Bar et al. 2016 IEEE International Conference on Software Science, Technology and Engineering (SWSTE), Beer Sheva, Israel, 23–24 June 2016. 2016. URL: https://doi.org/10.1109/swste.2016.13 (date of access: 06.12.2023).

66. Jha S., Sheyner O., Wing J. Two formal analyses of attack graphs. 15th IEEE Computer Security Foundations Workshop CSFW-15, Cape Breton, NS, Canada. URL: https://doi.org/10.1109/csfw.2002.1021806 (date of access: 06.12.2023).

67. Cloud security alliance. The Treacherous Twelve - Cloud Computing Top Threats in 2016. URL: https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf (date of access: 06.12.2023).

68. Patcha A., Park J.-M. An overview of anomaly detection techniques: existing solutions and latest technological trends. Computer networks. 2007. Vol. 51, no. 12. P. 3448–3470. URL: https://doi.org/10.1016/j.comnet.2007.02.001 (date of access: 06.12.2023).

69. Kanchanapokin S., Boonkrong S. Analysis of Organizational Vulnerability using Social Network Analysis and Attack Graph. GSTF Journal on Computing (JoC). 2016. Vol. 5, no. 1. URL: https://doi.org/10.7603/s40601-016-0001-3 (date of access: 06.12.2023).

70. An analysis of security issues for cloud computing / K. Hashizume et al. Journal of Internet Services and Applications. 2013. Vol. 4, no. 1. P. 5. URL: https://doi.org/10.1186/1869-0238-4-5 (date of access: 06.12.2023).

71. Hey, you, get off of my cloud / T. Ristenpart et al. the 16th ACM conference, Chicago, Illinois, USA, 9–13 November 2009. New York, New York, USA, 2009. URL: https://doi.org/10.1145/1653662.1653687 (date of access: 06.12.2023).

72. Ross S. M. Introduction to probability models. 6th ed. San Diego, CA : Academic Press, 1997. – 669 p.

73. Cybersecurity framework. *NIST*. URL: https://www.nist.gov/cyberframework (date of access: 03.12.2023).

74. Управління ризиками в проектах. Система електронного забезпечення навчання ЗНУ. URL: https://moodle.znu.edu.ua/pluginfile.php/777709/mod_resource/content/0/TEMA%2011_УПРАВЛІННЯ%20РИЗИКАМИ%20В%20ПРОЕКТАХ.pdf (дата звернення: 10.09.2023).

75. ISO 31000 – менеджмент рисков. ISO. URL: https://www.iso.org/ru/iso-31000-risk-management.html (дата звернення: 03.12.2021).

76. Cox L. A. Risk analysis of complex and uncertain systems. Boston, MA: Springer US, 2009. URL: https://doi.org/10.1007/978-0-387-89014-2 (date of access: 10.09.2023).

77. The role of big data in official statistics – UN global pulse. UN Global Pulse – Big data for development and humanitarian action. URL: https://www.unglobalpulse.org/2016/03/the-role-of-big-data-in-official-statistics/ (date of access: 10.09.2023).

78. Як зменшити ризики кіберзагроз, спрямованих проти інформаційної безпеки компаній. Юридичні послуги, адвокати | Василь Кісіль і Партнери. URL:

https://vkp.ua/publication/yak_zmenshiti_riziki_kiberzagroz_spryamovanikh_proti_informatsiynoi_bezpeki_kompaniy (дата звернення: 10.09.2023).

79. Vulnerability Statistics Report 2023. Edgescan. URL: https://www.edgescan.com/intel-hub/stats-report/ (date of access: 22.06.2023).

80. Тема 11. Управління ризиками в проектах. *Система електронного забезпечення навчання ЗНУ*. URL: https://moodle.znu.edu.ua/pluginfile.php/777709/mod_resource/content/0/ТЕМА%2011_УПРАВЛІННЯ%20РИЗИКАМИ%20В%20ПРОЕКТАХ.pdf (дата звернення: 03.12.2023).

81. Еськов А. Структурирование рисков и решений при использовании BigData для получения официальной статистики. *Хабр*. URL: https://habr.com/ru/post/494044/ (дата звернення: 03.12.2021).

82. https://jurliga.ligazakon.net/. Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX | ЮРЛІГА. *ЮРЛІГА*. URL: https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix (дата звернення: 03.12.2023).

83. Разработка основы стратегии анализа рисков для оценки воздействия в системах управления информационной безопасностью: пример из индустрии ИТ-консалтинга. Часть 2 | TIC - TUV Austria сертифікація. *TIC - TUV Austria сертифікація*. URL: https://tic-ua.com/articles/razrabotka-osnovy-strategii-analiza-riskov-dlya-oczenki-vozdejstviya-v-sistemah-upravleniya-informaczionnoj-bezopasnostyu-primer-iz-industrii-it-konsaltinga-chast-2/ (дата звернення: 03.12.2021).

84. Этапы статистического исследования и риски. URL: https://cyberleninka.ru/article/n/etapy-statisticheskogo-issledovaniya-i-riski/viewer (дата звернення: 03.12.2021).

85. CVE security vulnerability database. Security vulnerabilities, exploits, references and more. CVE security vulnerability database. Security vulnerabilities, exploits, references and more. URL: https://www.cvedetails.com/ (date of access: 28.07.2023).

86. Kuz V. Risk management of critical information infrastructure: threats-vulnerabilities-consequences. Theoretical and applied cybersecurity. 2023. Vol. 5, no. 2. URL: https://doi.org/10.20535/tacs.2664-29132023.2.280377 (date of access: 02.12.2023).

87. A review of cyber security risk assessment methods for SCADA systems / Y. Cherdantseva et al. Computers & security. 2016. Vol. 56. P. 1–27. URL: https://doi.org/10.1016/j.cose.2015.09.009 (date of access: 08.12.2023).

88. Baiardi F., Telmon C., Sgandurra D. Hierarchical, model-based risk management of critical infrastructures. Reliability Engineering & System Safety. 2009. Vol. 94, no. 9. P. 1403–1415. URL: https://doi.org/10.1016/j.ress.2009.02.001 (date of access: 08.12.2023).

89. Eling M., Wirfs J. What are the actual costs of cyber risk events?. European journal of operational research. 2019. Vol. 272, no. 3. P. 1109–1119. URL: https://doi.org/10.1016/j.ejor.2018.07.021 (date of access: 08.12.2023).

90. Information assurance: Dependability and security in networked systems / Y. Qian et al. Amsterdam : Elsevier/Morgan Kaufmann, 2007. – 537 p.

91. Automated generation and analysis of attack graphs / O. Sheyner et al. 2002 IEEE Symposium on Security and Privacy, Berkeley, CA, USA. URL: https://doi.org/10.1109/secpri.2002.1004377 (date of access: 29.12.2023).

92. Jha S., Sheyner O., Wing J. Two formal analyses of attack graphs. 15th IEEE Computer Security Foundations Workshop CSFW-15, Cape Breton, NS, Canada. URL: https://doi.org/10.1109/csfw.2002.1021806 (date of access: 29.12.2023).

93. Kolegov D. N. MODELING NETWORK COMPUTER SYSTEMS WITH VULNERABILITIES. Prikladnaya diskretnaya matematika. 2009. No. 5. P. 91–99. URL: https://doi.org/10.17223/20710410/5/10 (date of access: 30.12.2023).

94. Keramati M., Akbari A. An attack graph based metric for security evaluation of computer networks. 2012 Sixth International Symposium on Telecommunications (IST), Tehran, Iran, 6–8 November 2012. 2012. URL: https://doi.org/10.1109/istel.2012.6483149 (date of access: 30.12.2023).

95. Trost R. Practical intrusion analysis: Prevention and detection for the twenty-first century. Upper Saddle River, NJ : Addison-Wesley, – 2009.

96. Креневич А. П. Алгоритми і структури даних. URL: https://www.mechmat.univ.kiev.ua/wp-content/uploads/2021/09/pidruchnyk-alhorytmy-i-struktury-danykh.pdf (дата звернення: 02.01.2024).

97. Архипов О.Є. Вступ до теорії ризиків: інформаційні ризики : моногр. – К.: Нац. акад. СБУ, 2015. – 248 с.

98. Архипов О.Є., Муратов О.Є., Бровко В.Д. Основи теорії ризиків: навчальний посібник – К.: НА СБ України, 2019. – 267 с.

99. Інформаційне та соціально-правове моделювання : посібник / Д. В. Ланде, В. М. Фурашев ; за заг. ред. Д.В. Ланде. - Київ-Одеса : Фенікс, 2021. – 276 с. ISBN 978-966-928-791-5

100. Levenchuk B. Liudmyla, Vira G. Huskova, and Petro I. Bidyuk. "ЙМОВІРНІСНЕ МОДЕЛЮВАННЯ ОПЕРАЦІЙНИХ РИЗИКІВ." KPI Science News 3 (2021): 26-37.

101. Kuznietsova Nataliia, and Petro Bidyuk. "Adaptive Approach to Building Risk Models of Financial Systems." ITS. 2020.

102. Mokhor V., Gonchar S., Dybach O. Methods for the Total Risk Assessment of Cybersecurity of Critical Infrastructure Facilities. Nuclear and Radiation Safety. 2019. No. 2(82). P. 4–8. URL: https://doi.org/10.32918/nrs.2019.2(82).01 (date of access: 26.02.2024).

103. Мохор В., Цуркан В. Методологія побудови систем управління інформаційною безпекою. Ukrainian information security research journal. 2022. Т. 23, № 4. С. 200–211.

104. Літвінчук, Ірина and Коршун, Наталія Володимирівна and Ворохоб, Максим Віталійович (2020) Спосіб оцінювання інтегрованих систем безпеки на об’єкті інформаційної діяльності Кібербезпека: освіта, наука, техніка, 2 (10). pp. 135-143.

105. Літвінчук, Ірина and Корчомний, Руслан and Коршун, Наталія Володимирівна and Ворохоб, Максим Віталійович (2020) Підхід до

оцінювання ризиків інформаційної безпеки для автоматизованої системи класу «1» Кібербезпека: освіта, наука, техніка, 2 (10). pp. 98-112.

106. Lande D., Dmytrenko O., Fu M., et al. Algorithm for determining the mutual impact of nodes in weighted directed graphs. Soft Comput 25, 1465–1478 (2021). https://doi.org/10.1007/s00500-020-05232-9

107. Ланде Д. В., Страшной Л., Балагура І. В. Метод формування та кластеризації кореляційних мереж понять. Реєстрація, зберігання і обробка даних. 2021. Т. 23, № 2. С. 27–36.

108. Толюпа С., Пархоменко І., Штаненко С. Модель системи протидії вторгненням в інформаційних системах. Information and communication technologies, electronic engineering. 2021. Т. 1, № 1. С. 39–50. URL: https://doi.org/10.23939/ictee2021.01.039 (дата звернення: 28.02.2024).

109. PROTECTION OF STATE MANAGEMENT OF CRITICAL INFRASTRUCTURE OBJECTS UNDER THE INFLUENCE OF CYBER ATTACKS / S. Toliupa et al. Information and communication technologies, electronic engineering. 2022. Vol. 2, no. 2. P. 33–41. URL: https://doi.org/10.23939/ictee2022.02.033 (date of access: 28.02.2024).

ДОДАТОК А

Список основних публікацій здобувачки за темою дисертації

1. Полуциганова В. І., Смирнов С. А. Методологія побудови основних метрик q-аналізу та їх застосування. *Системні дослідження та інформаційні технології*. 2019. № 3. С. 76–88. URL: https://doi.org/10.20535/srit.2308-8893.2019.3.07 (date of access: 10.11.2023).

2. Polutsyganova V., Smirnov S. The inverse problem of Q-analysis of complex systems structure in cyber security. *Theoretical and applied cybersecurity*. 2023. Vol. 4, no. 1. URL: https://doi.org/10.20535/tacs.2664-29132022.1.274123 (date of access: 10.11.2023).

3. Polutsyhanova V. I. System construction of cybersecurity vulnerabilities with Q-analysis. *Theoretical and applied cybersecurity*. 2023. Vol. 5, no. 1. URL: https://doi.org/10.20535/tacs.2664-29132023.1.285430 (date of access: 08.11.2023).

4. Polutsyhanova V. I. Vulnerability classification using Q-analysis. *Theoretical and applied cybersecurity*. 2023. Vol. 5, no. 2. P. 56–61. URL: https://doi.org/10.20535/tacs.2664-29132023.2.285431 (date of access: 08.11.2023).

5. Медведенко (Полуциганова) В. І., Смирнов С. А. Використання q-аналізу для дослідження зв'язків у банківських системах. *XV Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики»*: Всеукр. науково-практ. конференція студентів, аспірантів та молодих вчен., м. Київ, 25–27 трав. 2017 р. Київ, 2017. С. 44–46.

6. Медведенко (Полуциганова) В. І., Смирнов С. А. Використання алгоритмів q-аналізу на прикладі банківської системи. *XVI Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики»*:

Всеукр. науково-практ. конференція студентів, аспірантів та молодих вчен., м. Київ, 26–27 квіт. 2018 р. Київ, 2018. С. 33–36.

7. Polutsyhanova V. The inverse problem of q-analysis. *XVIII Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики»:* Всеукр. науково-практ. конференція студентів, аспірантів та молодих вчен., м. Київ, 12–13 трав. 2020 р. С. 113–115.

8. Полуциганова В. І., Смирнов С. А. The inverse problem of Q-analysis of comple x systems structure. *Інформаційні технології та безпека матеріали XXII міжнародної науково-практичної конференції випуск*, м. Київ, 2021. С. 114–118.

9. Полуциганова В. І., Смирнов С. А. Оцінювання ризиків складних систем з використання методів Q-аналізу. *Інформаційні технології та безпека матеріали XXIII міжнародної науково-практичної конференції випуск*, м. Київ, 2022. С. 51–52.

10. Полуциганова В. І., Смирнов С. А. Structure of vulnerability in complex systems and risk assessment// МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ «Виклики і загрози для критичної інфраструктури» 21-22 березня 2023 р. м. Київ, Україна. С. 334-335.

11. Полуциганова В. І., Смирнов С. А. Оцінка ризиків в кібербезпеці за допомогою Q-аналізу. *XXI Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики»*: Всеукр. науково-практ. конференція студентів, аспірантів та молодих вчен., м. Київ, 12–13 трав. 2023 р. Київ, 2017. С. 172–173.

12. Polutsyhanova V. I., Smirnov S. A. Assessing cybersecurity risk with Q-analysis. *Всеукраїнська науково-практична конференція «Theoretical and Applied Cybersecurity» (TACS-2023)*, Kyiv, 26 May 2023. P. 57 – 60.

ДОДАТОК Б

АКТИ ВПРОВАДЖЕННЯ І ВИКОРИСТАННЯ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЇ

ЗАСТУПНИК СЕКРЕТАРЯ
РАДИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ
вул. Петра Болбочана, 8, м. Київ, 01601, телефон: (044) 255-06-50, телефакс: (044) 255-05-85

_____ № _____
_____

З А Т В Е Р Д Ж У Ю
Заступник Секретаря
Ради національної безпеки і
оборони України

С.В.ДЕМЕДЮК
«_____» 20___ року

А К Т
впровадження результатів дисертаційного дослідження
Полуциганової Вікторії Ігорівни

Комісія у складі працівників Апарату РНБО України: голови комісії – керівника служби з питань інформаційної безпеки та кібербезпеки Ткачук Н.А. та членів комісії: державного експерта управління з питань екологічної та енергетичної безпеки служби з питань економічної безпеки Чумаченко С.М. та державного експерта управління з питань інформаційної безпеки служби з питань інформаційної безпеки та кібербезпеки Скибуна О.Ж., склала цей акт впровадження результатів дисертаційного дослідження у діяльність Апарату Ради національної безпеки і оборони України, підготовлених Полуциганową В.І. – асистентом кафедри інформаційної безпеки Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», щодо методу оцінки ризику на основі аналізу структури зв'язків загроз та вразливостей у кіберсистемах.

У рамках дослідження Полуциганową В.І. на основі удосконалення процедури байєсової оцінки ризику визначено узагальнений метод розрахунку поліноміальної функції середнього ризику загроз для кіберсистеми суб'єкта забезпечення кібербезпеки в залежності від сумісності реалізації вразливостей як структурних компонентів загроз. Цей метод також ураховує структуру

симплеціального комплексу, створеного на основі системи зв'язків між уразливостями й загрозами, та складену функцію втрат.

Наукові напрацювання та пропозиції використані під час підготовки матеріалів до засідання Ради національної безпеки і оборони України з питання «Про стан справ у енергетичній сфері» (протокольне рішення від 22 жовтня 2021 року № 33), рішення Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України (далі – НКЦК) (протокол від 25 жовтня 2021 № 18 дск), а також у процесі розроблення Загальних правил обміну інформацією про кіберінциденти, затверджених рішенням НКЦК від 09 лютого 2023 (протокол № 21).

Комісія вважає, що представлені Полуциганową Вікторією Ігорівною пропозиції, підготовлені на основі наукового дослідження, мають теоретичну та практичну значимість для вдосконалення державної політики з питань національної безпеки у сфері забезпечення кібербезпеки, насамперед щодо підвищення рівня кіберзахисту інформаційно-комунікаційних систем об'єктів критичної інфраструктури, зокрема паливно-енергетичного сектору.

Голова комісії:

Керівник служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО України, кандидат юридичних наук **Н. ТКАЧУК**

Члени комісії:

Державний експерт управління з питань екологічної та енергетичної безпеки служби з питань економічної безпеки Апарату РНБО України, доктор технічних наук **С. ЧУМАЧЕНКО**

Державний експерт управління з питань інформаційної безпеки служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО України, кандидат наук з державного управління **О. СКИБУН**

ЗАТВЕРДЖУЮ
Проректор з навчальної роботи
Національного
технічного університету України
«Київський політехнічний інститут
імені Ігоря Сікорського»
Анатолій МЕЛЬНИЧЕНКО
«19» лютого 2024 р.

АКТ

впровадження результатів дисертаційного дослідження асистентки кафедри Інформаційної безпеки навчально-наукового фізико-технічного інституту Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» Полуциганової Вікторії Ігорівни на тему «Метод оцінки ризику на основі аналізу структури зв'язків загроз та вразливостей у кіберсистемах» на здобуття ступеня доктора філософії.

Комісія у складі: голова -- завідувач кафедри ІБ КПІ ім. Ігоря Сікорського, д.т.н. проф. Ланде Д.В.; члени комісії – професор кафедри ІБ КПІ ім. Ігоря Сікорського, д.т.н. проф. Мачуський Є.А., доцент кафедри ІБ КПІ ім. Ігоря Сікорського, к.т.н. доц. Стьопочкіна І. В. цим Актом засвічує, що результати дисертаційного дослідження Полуциганової Вікторії використані співробітниками кафедри ІБ КПІ ім. Ігоря Сікорського при підготовці та викладанні курсів лекцій «Рішення в умовах невизначеності та ризику», «Проблеми кібербезпеки критичної інфраструктури», «Математичні моделі кібербезпеки». Зокрема впроваджено огляд та застосування алгоритмів аналізу та синтезу симплеціальних комплексів вразливостей та загроз кіберсистем на основі Q-аналізу, структурна класифікація загроз та вразливостей кіберсистем, метод розрахунку ризику з врахуванням структури зв'язків загроз та вразливостей у кіберсистемах; розроблено завдання для практичних занять по відповідних темах.

Голова комісії
д.т.н. проф. Дмитро ЛАНДЕ

Члени комісії
к.т.н. доц. Ірина СТЬОПОЧКІНА

д.т.н. проф. Євгеній МАЧУСЬКИЙ

Реєстраційна картка НДДКР

Державний реєстраційний номер: 0124U001957

Відкрита

Дата реєстрації: 21-02-2024

Статус виконавця: 17 - головний виконавець

1. Загальні відомості

Підстава для проведення робіт: 43 - власна ініціатива (якщо робота виконується з власної ініціативи за кошти виконавця НДР або безкоштовно)

КПКВК:

Напрям фінансування: 2.1 - фундаментальні дослідження

Джерела фінансування

7706 - безплатно (договір про науково-технічне співробітництво, тощо)

Загальний обсяг фінансування (тис. грн.): 0.000

У тому числі по роках (тис. грн.):

Рік	Фінансування

2. Замовник

Назва організації: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код ЄДРПОУ/ІПН: 02070921

Адреса: проспект Берестейський, буд. 37, м. Київ, 03056, Україна

Підпорядкованість: Міністерство освіти і науки України

Телефон: 380442367989

Телефон: 380442044862

Телефон: 380442049494

E-mail: mail@kpi.ua

WWW: https://kpi.ua/

3. Виконавець

Назва організації: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код ЄДРПОУ/ІПН: 02070921

Підпорядкованість: Міністерство освіти і науки України

Адреса: проспект Берестейський, буд. 37, м. Київ, 03056, Україна

Телефон: 380442367989

Телефон: 380442044862

Телефон: 380442049494

E-mail: mail@kpi.ua

WWW: https://kpi.ua/

4. Співвиконавець

5. Науково-технічна робота

Назва роботи (укр)

Підтримка прийняття рішень в умовах невизначеності та конкурентної взаємодії

Назва роботи (англ)

Decision-making support in conditions of uncertainty and competitive interaction

Мета роботи (укр)

Розробка методів моделювання та підтримки прийняття рішень в ситуаціях: 1) структурно-складної взаємодії; 2) конкурентної взаємодії; 3) наявності рефлексивних впливів

Мета роботи (англ)

Development of modeling methods and decision-making support in situations of: 1) structurally complex interaction; 2) competitive interaction; 3) the presence of reflexive influences

Пріоритетний напрям науково-технічної діяльності:

Стратегічний пріоритетний напрям інноваційної діяльності: Розвиток сучасних інформаційних, комунікаційних технологій, робототехніки

Вид роботи: 39 - фундаментальна

Очікувані результати: Методи, теорії, Аналітичні матеріали

Галузь застосування: Дослідження й експериментальні розробки у сфері природничих і технічних наук

Експерти

6. Етапи виконання

Номер	Початок	Закінчення	Звітний документ	Назва етапу
1	01.2024	12.2026	Остаточний звіт	Задачі розподілу ресурсів для інформаційного протиборства та захисту від кібератак. Рефлексивні моделі багатостороннього конкурентного протиборства.

7. Індекс УДК тематичних рубрик НТІ

Коди тематичних рубрик НТІ: 28.29.67.37, 28.29.04, 28.29.05, 27.47.19, 28.17.27, 28.17.31

Індекс УДК: , 519.81;519.816, 519.83, 519.8 , 519.711.3 , 519.711 , 519.8, 519.81, 519.816, 519.83, 519.711.3, 519.711

8. Заключні відомості

Керівник організації:

Пасічник Віталій Анатолійович (д. т. н., професор)

Керівники роботи:

Смирнов Сергій Анатолійович

Відповідальний за подання документів: Собецька Анна (Тел.: +38 (067) 266-60-15)

Керівник відділу реєстрації наукової діяльності УкрІНТЕІ

Юрченко Т.А.