МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРНІГІВСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»

Кваліфікаційна наукова
праця на правах рукопису

ВОЙЦЕХОВСЬКА МАРІЯ МИХАЙЛІВНА

УДК 004.056:658(043.5)

Д И С Е Р Т А Ц І Я

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ОЦІНЮВАННЯ РІВНЯ КУЛЬТУРИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

122 – Комп’ютерні науки

12 – Інформаційні технології
галузь знань

Подається на здобуття наукового ступеня доктора філософії

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

_____ Войцеховська Марія Михайлівна
підпис

Науковий керівник Литвинов Віталій Васильович
доктор технічних наук, професор
Дорош Марія Сергіївна
доктор технічних наук, доцент

Чернігів – 2020

АНОТАЦІЯ

Войцеховська Марія Михайлівна. Інформаційна технологія оцінювання рівня культури інформаційної безпеки організації. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 122 – «Комп'ютерні науки» (12 – «Інформаційні технології»). – Національний університет «Чернігівська політехніка», МОН України, Чернігів, 2020.

В роботі вирішено актуальне *наукове завдання* з розробки моделей та методів інформаційних процесів оцінювання рівня культури інформаційної безпеки організації, які дозволять автоматизувати систему визначення поточного рівня культури інформаційної безпеки організації з врахуванням персональних показників співробітників, актуальних ризиків в галузі інформаційної безпеки та нормативних вимог до ведення безпечної діяльності організації в умовах інформатизації.

Метою дисертаційного дослідження є розробка моделей та методів інформаційної технології комплексного оцінювання рівня культури інформаційної безпеки організації з урахуванням особливостей людино-машинної взаємодії, для підтримки прийняття рішень щодо забезпечення відповідного показника безпеки організації.

Для досягнення поставленої мети були сформульовані такі *завдання дослідження:*

1) Сформувати перелік первинних показників рівня культури інформаційної безпеки організації та її індикаторів.
2) Розробити модель інформаційних процесів обчислення рівня культури інформаційної безпеки організації.
3) Розробити елементи інформаційної технології визначення рівня культури інформаційної безпеки організації.

4) Провести експериментальне дослідження щодо збору та обробки первинної інформації для інформаційної технології оцінювання рівня культури інформаційної безпеки організації.

Об'єкт дослідження – інформаційні процеси визначення культури інформаційної безпеки організації.

Предмет дослідження – методи, моделі та інформаційна технологія комплексної оцінки рівня культури інформаційної безпеки організації з врахуванням особливостей людино-машинної взаємодії.

Основні результати дослідження та наукова новизна роботи полягають в тому, що визначено роль культури інформаційної безпеки у загальній системі інформаційної безпеки організації, враховуючи особливості професійної діяльності та пов’язану з обов’язками взаємодію з інформаційною системою, внутрішнім інформаційним простором та зовнішнім середовищем.

Враховуючи складність формалізації предметної області, було запропоновано скористатися математичним апаратом м’яких обчислень, а саме обчисленнями на основі логіки антонімів, нечіткої логіки та нечіткої кластеризації.

Розроблена модель визначення вимог до рівня культури інформаційної безпеки, яка враховує навички користування технічною складовою системи інформаційної безпеки організації та власне персональні аспекти, що стосуються безпечної поведінки при роботі з інформаційними ресурсами.

Запропонована модель оцінки рівня персональної культури інформаційної безпеки співробітників організації. Оцінювання рівня персональної культури інформаційної безпеки за допомогою ієрархічної системи нечіткого логічного виводу дозволяє сформувати комплект індивідуальних анкет з врахуванням особливостей професійної діяльності співробітників та їх посадових обов’язків.

Для обрахування загального впливу культури інформаційної безпеки персоналу на рівні безпеки структурного підрозділу та організації

запропонована математична модель, яка враховує особливості професійної діяльності працівників.

На основі аналізу міжнародних стандартів ISO/IEC 27001:2015, ISO/IEC 27032:2016 та наробок з формування культури безпеки на об’єктах критичної інфраструктури запропоновано ієрархічну нечітку модель визначення рівня культури інформаційної безпеки організації, яка дозволяє формалізувати процес обчислення з подальшим наданням рекомендацій щодо вибору заходів, спрямованих на підвищення культури інформаційної безпеки.

Запропонована модель визначення структурних підрозділів, в яких має бути впроваджена культура інформаційної безпеки, а також вибору проектного або процесного підходів для впровадження комплексу заходів для оцінки рівня КІБ, його підвищення та подальшого закріплення в якості корпоративного стандарту.

Вперше розроблена модель інформаційного процесу оцінювання рівня КІБ організації, яка на відміну від існуючих, містить аспекти людино-машинної взаємодії і враховує фактори персональної культури безпеки учасників процесу.

Вперше розроблено метод автоматизованої оцінки рівня КІБ організації, який на відміну від існуючих, базується на використанні нечіткої логіки на основі алгоритму Мамдані, і дозволяє виконувати оцінку поетапно на різних організаційних рівнях.

Дістала подальшого розвитку структура системи ІБ організації за рахунок включення факторів персональної КІБ, що дозволяє враховувати вплив людського чинника на загальну систему безпеки організації.

Дістав подальшого розвитку метод оцінки рівня персональної КІБ на основі компетентнісного підходу за рахунок використання логіки антонімів, що забезпечує підвищення ефективності проведення таких оцінок.

Практичне значення отриманих результатів полягає в тому, що наведені вище наукові результати у своїй сукупності утворюють нову інформаційну технологію оцінки рівня культури інформаційної безпеки

організації. Запропонована інформаційна технологія може бути корисною для керівників ІБ-підрозділів та організацій для підтримки впроваджених систем забезпечення інформаційної безпеки. Розроблені бізнес-процеси та архітектура можуть бути використані як основа для розроблення власних систем моніторингу культури інформаційної безпеки; модель оцінки персональної культури інформаційної безпеки – при призначенні певних рівнів доступу до інформаційних систем; моніторингу поточного рівня культури інформаційної безпеки персоналу, структурного підрозділу та саме організації для визначення прогалин в обізнаності та компетенцій в галузі ІБ; формуванні команд реагування на інциденти, тощо.

Дана інформаційна технологія має наступне практичне втілення.

Модель нечіткого логічного виводу дає можливість проводити оцінку рівня культури інформаційної безпеки без спеціальних навичок, що значно розширює можливості її використання в неспеціалізованих організаціях.

Забезпечення швидкого самооцінювання виконується за допомогою розробленої автоматизованої телефонної системи (чатботу).

Результати дисертаційних досліджень впроваджені:

– при виконанні міжнародного наукового проекту «Cyber Rapid Analysis for Defense Awareness of Real-time Situation – CyRADARS» за грантом NATO SPS, (grant agreement number: G5286), науково-дослідних робіт Національного університету «Чернігівська політехніка» «Моделі та методи оцінювання конвергенції систем компетентностей фахівців з використанням технологій штучного інтелекту» (№0120U101929), «Розробка моделей та методів захисту системи від зовнішніх атак з використанням технологій штучного інтелекту» (№0120U101931) та «Розвиток базового моделюючого комплексу мережі ситуаційних центрів державних органів сектору безпеки і оборони України в інтересах захисту критичної інфраструктури держави та кібербезпеки» (№0119U000058т) Інституту проблем математичних машин і систем Національної академії наук України;

– на ПАТ «ЧЕЗАРА» під час впровадження тестування персоналу на стадії підбору та приймання на роботу на предмет виявлення базового рівня персональної культури інформаційної безпеки;
– в Державному науково-випробувальному інституті випробувань та сертифікації озброєння та військової техніки при розробці документації інформаційних систем «Інформаційна система з доступом до мережі Internet (ІСД-Internet)» та «Система електронного документообігу (СЕДО)»;
– у навчальному процесі Чернігівського національного технологічного університету (Національного університету «Чернігівська політехніка») при проведенні лекцій та лабораторних робіт з дисципліни «Моделі та системи штучного інтелекту» – в процесі навчання бакалаврів спеціальності 121 – «Інженерія програмного забезпечення» на кафедрі інформаційних технологій та програмної інженерії.

Ключові слова: культура, персонал, організація, обізнаність, інформаційна безпека, організаційна культура, експерт, інформаційна система, інформаційна технологія.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Dorosh M., Trunova O., Itchenko D., Voitsekhovska M., Dvoieglazova M. The study of participants' values convergence on the example of international scientific project on cyber security. *Eastern-European Journal of Enterprise Technologies,* 2016. Vol. 6/3 (84). P. 4-10. DOI: 10.15587/1729-4061.2016.85215 (SCOPUS). (0,8 ум. друк. арк.) (Особистий внесок здобувача: формування цінностей у напрямку інформаційної безпеки учасників проекту). (0,1 ум. друк. арк.).

2. Dorosh M., Voitsekhovska M., Balchenko I. Research and Determination of Personal Information Security Culture Level Using Fuzzy Logic Methods. *Advances in Intelligent Systems and Computing*. Springer, Cham. *P. II : Advances in Computer Science for Engineering and Education.* - 2020. – Vol. 938. – P. 503–512. DOI https://doi.org/10.1007/978-3-030-16621-2_47 (SCOPUS, SpringerLink). (1,16 ум. друк. арк.). (Особистий внесок здобувача: модель оцінки рівня персональної культури інформаційної безпеки на основі ієрархічної нечіткої моделі, а також результати експериментального дослідження). (0,8 ум. друк. арк.).

3. Shkarlet S., Lytvynov V., Dorosh M., Trunova E., Voitsekhovska M. The Model of Information Security Culture Level Estimation of Organization. *Advances in Intelligent Systems and Computing*. Springer, Cham. *P. II.* : *Mathematical Modeling and Simulation of Systems*. – 2020. – Vol. 1019. – P. 249-258. DOI https://doi.org/10.1007/978-3-030-25741-5_25 (SCOPUS, SpringerLink). (1,16 ум. друк. арк.). (Особистий внесок здобувача: модель оцінки рівня культури інформаційної безпеки організації). (0,7 ум. друк. арк.).

4. Lytvynov V., Dorosh M., Bilous I., Voitsekhovska M., Nekhai V. Development of the automated information system for organization's information security culture level assessment. *Technical sciences and technologies*. 2020. № 1 (19). P. 124-132. DOI: 10.25140/2411-5363-2020-1(19)-124-132. (Фаховий журнал). (1,0 ум. друк. арк.). (Особистий внесок здобувача: архітектура, функціональна модель в нотації IDEF0 та логічна модель бази даних, що входить до інформаційної системи підтримки інформаційної технології оцінювання рівня КІБ організації.). (0,8 ум. друк. арк.).

5. Shkarlet S., Dorosh M., Druzhynin O., Voitsekhovska M., Bohdan I. (2021) Modeling of Information Security Management System in the Project. *MODS*

2020. Advances in Intelligent Systems and Computing. Springer, Cham. *P. II. Mathematical Modeling and Simulation of Systems.* – 2021. – Vol. 1265. – P. 364-376. DOI https://doi.org/10.1007/978-3-030-58124-4_35 (SCOPUS, SpringerLink). (1,4 ум. друк. арк.). (Особистий внесок здобувача: модель формування культури інформаційної безпеки під час проектної діяльності в рамках методології PMBoK). (0,4 ум. друк. арк.).

Наукові праці, які засвідчують апробацію матеріалів дисертації:

6. Литвинов В.В., Трунова О.В., Войцеховська М.М. Модель культури інформаційної безпеки організації. *Перспективні напрями захисту інформації* : зб. тез доп. другої Всеукр. наук.-практ. конф. (м. Одеса, 03-07 верес. 2017 р.). – Одеса, 2016. – С. 47-50. (0,2 ум. друк. арк.). (Особистий внесок здобувача: обґрунтування культури інформаційної безпеки як одного з аспектів корпоративної культури організації).

7. Литвинов В.В., Трунова О.В., Войцеховська М.М. Формування і підвищення культури інформаційної безпеки організації. *Створення та модернізація озброєння і військової техніки в сучасних умовах* : зб. тез доп. шістнадцятої наук.-тех. конф. (м. Чернігів, 08-09 верес. 2016 р.). – Чернігів, 2016. – С. 163-164. (0,2 ум. друк. арк.). (Особистий внесок здобувача: визначення засобів по формуванню КІБ організації).

8. Трунова О.В., Войцеховська М.М. Використання логіки антонімів при оцінці стану культури інформаційної безпеки організації. *Проблеми зняття з експлуатації об'єктів ядерної енергетики та відновлення навколишнього середовища INUDECO 2017* : матеріали другої Міжнар конференції (м. Славутич, 25-27 квіт. 2017 р.). – Славутич, 2017. – С. 276-280. (0,3 ум. друк. арк.). (Особистий внесок здобувача: обґрунтування застосування формального апарату логіки антонімів для оцінки рівня сформованості компетенцій в галузі інформаційної безпеки ІТ-фахівців).

9. Войцеховська М.М. Культурно-антропологічні чинники інформаційної безпеки в умовах постіндустріального суспільства. *Юність науки – 2017: соціально-економічні та гуманітарні аспекти розвитку суспільства* : зб. тез доп. Міжнар. наук.-практ. конф. студ., аспір. і молод. вчених (м. Чернігів, 25-27 квіт. 2017 р.). – Чернігів : ЧНТУ, 2017. – С. 452-454. (0,3 ум. друк. арк.).

10. Войцеховська М.М. Логіка антонімів при оцінці компетенцій в галузі інформаційної безпеки. *Новітні технології у науковій діяльності і навчальному процесі* : зб. тез доп. Всеукр. наук.-практ. конф. студ., аспір. та молод. вчених (м. Чернігів, 19-20 квіт. 2017 р.) – Чернігів : ЧНТУ, 2017. – С. 47-48. (0,1 ум. друк. арк.).

11. Трунова О.В., Войцеховська М.М. Модель визначення рівня сформованості компетенцій ІТ-фахівця. *Математичне та імітаційне моделювання систем. МОДС 2017* : зб. тез доп. дванадцятої Міжнар. наук.-практ. конф. (м. Чернігів, 26-29 черв. 2017 р.) – Чернігів : ЧНТУ, 2017. – С. 376-378. (0,2 ум. друк. арк.). (Особистий внесок здобувача: модель визначення рівня сформованості ІБ-компетенцій ІТ-фахівця).

12. Войцеховська М. М., Дорош М. С. Використання експертної системи на базі нечіткої логіки для визначення рівня культури інформаційної безпеки організації. *Проблеми зняття з експлуатації об'єктів ядерної енергетики та відновлення навколишнього середовища (INUDECO 2018)* : зб. матеріалів ІІІ Міжнар. конф. (м. Славутич, 25-27 квіт. 2018 р.). – Чернігів : ЧНТУ, 2018. – С. 61-64. (0,2 ум. друк. арк.). (Особистий внесок здобувача: застосування нечіткої логіки для кількісно-якісної оцінки стану культури інформаційної безпеки співробітників).

13. Войцеховська М.М., Бальченко І.В. Застосування нечіткої ієрархічної системи для оцінки базової культури кібербезпеки користувача (Применение нечеткой иерархической системы для оценки базовой

культуры кибербезопасности пользователя). *Математичне та імітаційне моделювання систем. МОДС 2018* : зб. тез доп. тринадцятої Міжнар. наук.-практ. конф. (м. Чернігів, 25-29 червня 2018 р.). – Чернігів : ЧНТУ, 2018. – С. 339-341. (0,2 ум. друк. арк.). (Особистий внесок здобувача: модель ієрархічної нечіткої системи в Matlab Fuzzy Logic Designer).

14. Дорош М.С., Войцеховська М.М. Визначення рівня персональної культури інформаційної безпеки як складової загального показника безпеки корпоративних мереж. *Інформаційні технології та взаємодії (IT&I'2018)* : зб. тез доп. V Міжнар. наук.-практ. конф. (м. Київ, 20-21 листоп. 2018 р.). – Київ : КНУ ім. Т. Шевченка, 2018. – С. 267-268. (0,1 ум. друк. арк.). (Особистий внесок здобувача: модель визначення належного рівня КІБ працівників з врахуванням ІБ-ризику).

15. Дорош М.С., Войцеховська М.М. Впровадження культури інформаційної безпеки при управлінні проектами. *Безпека соціально-економічних процесів в кіберпросторі* : матеріали Всеукр. наук.-практ. конф. (м. Київ, 27 берез. 2019 р.) – Київ : КНТЕУ, 2019. – С. 175-176. (0,2 ум. друк. арк.). (Особистий внесок здобувача: обґрунтування впровадження КІБ при здійсненні проектної діяльності).

16. Дорош М.С., Войцеховська М.М., Дружинін О.О. Фактори безпеки при виборі інформаційних систем управління проектами. *Управління проектами у розвитку суспільства* : матеріали XVI міжнар. конф. (м. Київ, 17-18 трав. 2019 р.). – Київ, 2019. –С. 106-108. (0,2 ум. друк. арк.). (Особистий внесок здобувача: обґрунтування культури інформаційної безпеки як процесу проектної діяльності).

17. Дорош М.С., Нехай В.В., Войцеховська М.М. Архітектура інформаційної системи оцінки рівня культури інформаційної безпеки організації. *Математичне та імітаційне моделювання систем. МОДС*

2019 : зб. тез доп. Чотирнадцятої міжнар. наук.-практ. конф. (м. Чернігів, 24-26 черв. 2019 р.). – Чернігів : ЧНТУ, 2019. –С. 309-313. (0,3 ум. друк. арк.). (Особистий внесок здобувача: нечітка кластеризація як механізм формування анкет, архітектура інформаційної системи).

18. Dorosh M., Voitsekhovska M. Information Security Culture Wide-Scale Implementation Model. *Проблеми зняття з експлуатації об'єктів ядерної енергетики та відновлення навколишнього середовища (INUDECO 2020)* : зб. матеріалів IV Міжнар. конф. (м. Славутич, 27-29 квітня 2020 р.). – Чернігів : ЧНТУ, 2020. – С. 73-77. (0,3 ум. друк. арк.). (Особистий внесок здобувача: модель повномасштабного впровадження культури інформаційної безпеки).

ABSTRACT

Mariia Voitsekhovska. Information technology of assessing the level of information security culture of organization. – Qualifying scientific work on the rights of manuscript.

PhD thesis in Engineering Science under Specialty 122 – "Computer Sciences". –"Chernihiv Polytechnic" National University, Ministry of Education and Science of Ukraine, Chernihiv, 2020.

The thesis is devoted to solving the *current scientific problem* of developing an information technology to assess the level of information security culture of organization taking into account the personal information security culture of employees.

The thesis *purpose* is to develop models and methods of information technology for complex assessment of the level of information security culture of organization, taking into account the peculiarities of human-computer interaction, to support decision-making to ensure appropriate security.

To achieve this goal, the following *tasks* were formulated:

1) Form a primary indicators list of the information security culture level of the organization.
2) Develop a model of information processes for assessing the level of information security culture of the organization.
3) Develop elements of information technology to determine the level of information security culture of the organization.
4) Conduct an experimental study on the collection and processing of primary information for information technology to assess the level of information security culture of organization.

The object of research – information processes for assessing the information security culture of organization.

The subject of research – methods, models and information technology of complex assessment of the level of information security culture of the organization taking into account the peculiarities of human-computer interaction.

The main results of the research and scientific novelty of the work are follows.

The role of information security culture in the overall information security system of the organization is determined, taking into account the peculiarities of professional activity and related interaction with information system, internal information space and external environment.

Given the complexity of formalizing the subject area, it was proposed to use a soft computing mathematical apparatus, namely calculations based on the logic of antonyms, fuzzy logic and fuzzy clustering.

A model has been developed to set requirements for the level of competence in the field of information security, which takes into account the skills of using the technical component of the information security system of the organization and personal aspects related to safe behavior when working with information resources.

A model for assessing the level of personal information security culture of employees of the organization is proposed. Assessing the level of personal information security culture using a hierarchical system of fuzzy inference allows to create a set of individual questionnaires, taking into account the characteristics of professional activities of employees and their job responsibilities.

To evaluate the overall impact of the information security culture of personnel on the structural unit and organization level, a mathematical model is proposed, which takes into account the peculiarities of the professional activities of employees.

Based on the analysis of international standards ISO/IEC 27001:2015, ISO/IEC 27032:2016 and developments in the formation of security culture in critical infrastructure, a hierarchical fuzzy model for determining the level of information security culture of the organization is proposed, which allows to formalize the calculation process on the choice of measures aimed at improving the information security culture.

A model for determining a number of structural units in which information security culture should be implemented, as well as the choice of design or process approaches to implement a set of measures to assess the level of information security culture, increase it and further consolidate it as a corporate standard.

For the first time, a model of the information process of assessing the level of information security culture of the organization was developed, which, unlike the existing ones, contains aspects of human-compuetr interaction and takes into account the factors of personal safety culture of the participants.

For the first time, a method of automated assessment of the organization's information security culture level was developed, which, unlike the existing ones, is based on the use of fuzzy logic based on the Mamdani algorithm, and allows to perform assessment in stages at different organizational tiers.

The structure of the organization's information security system was further developed due to the inclusion of personal information security culture factors, which allows to take into account the influence of the human factor on the overall security system of the organization.

The method of assessing the level of personal information security culture on the basis of the competence approach through the use of the logic of antonyms was further developed, which provides an increase in the efficiency of such assessments.

The practical significance of the obtained results is forming a new information technology for assessing the level of information security culture of an organization. The offered information technology may be useful for IT managers and organizations to support implemented information security systems. Developed business processes and architecture can be used as a basis for developing their own systems for information security culture monitoring; model of assessment of personal information security culture may be useful in assigning certain levels of access to information systems; monitoring the current level of information security culture of the personnel, the structural unit and the organization overall to identify gaps in awareness and competence in the field of information security; formation of incident response teams, etc.

This information technology has the following practical embodiment.

The fuzzy inference model makes it possible to assess the level of information security culture without special skills, which significantly expands the possibilities of its use in non-specialized organizations.

Ensuring rapid self-assessment is performed using a developed automated telephone system (chatbot).

The results of the research are implemented:

- in carrying out the international research project «Cyber Rapid Analysis for Defense Awareness of Real-time Situation – CyRADARS» under NATO SPS grant (grant agreement number: G5286), Chernihiv Polytechnic National University research works: "Intelligent systems for estimation of higher education applicants' competency in Information Technology domain" (№0120U101929), "Intelligent information technology systems development for organization's network infrastructure cyber attacks protection" (№0120U101931); and research work "Development of the basic modeling complex of a network of situational centers of state bodies of the security and defense sector of Ukraine in the interests of protection of critical infrastructure of the state and cybersecurity" (№0119U000058t) of the Institute of Mathematical Machines and Systems Problems of the National Academy of Sciences of Ukraine;
- at PrJSC "CHEZARA" during the implementation of personnel testing at the stage of selection and employment to identify the basic level of personal information security culture;
- at State Research Institute of Testing and Certification of Weapons and Military Equipment when developing the documentation of information systems "Information system with Internet access (ISD-Internet)" and "Electronic document management system (EDMS)";
- to the education process in Chernihiv National University of Technology (National University “Chernihiv Polytechnics”) to the lectures and laboratory work on the course “Models and Systems of Artificial Intelligence” – in the teacing process for bachelors of Specialty 121 – “Software Engineering” at the Information Technology and Software Engineering department.

Keywords: culture, employee, organization, awareness, information security, corporate culture, expert, information system, information technology.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІБ – інформаційна безпека

БД – база даних

БП – база правил

КІБ – культура інформаційної безпеки

КМ – корпоративна мережа

ЛА – логіка антонімів

ЛОМ – локальна обчислювальна мережа

НЛ – нечітка логіка

ОС – операційна система

СЗІБ – система забезпечення інформаційної безпеки

СІ – соціальна інженерія

СНВ – система нечіткого виводу

СУІБ/СМІБ – система управління/менеджменту інформаційної системи

ФН – функція належності

ВСТУП

Актуальність теми дослідження. У сучасній ситуації одними з рушійних сил успішної бізнес-діяльності виступають технології, мобільність та доступність послуг. Інвестиції в інформаційні активи оцінюються нарівні з матеріальним капіталом, і захист цих інформаційних активів заслужено потребує посиленої уваги. Незважаючи на інтенсивний розвиток технічних засобів захисту інформації, на які власники та особи, відповідальні за інформаційні активи, покладаються в більшості випадків, працівники все ще залишаються не останнім фактором, що впливає на безпеку та цілісність інформаційних активів організації. Захищеність ресурсів, обчислювальної потужності, програмного забезпечення та інтересів користувачів все ще залежить від здатності персоналу протистояти зовнішнім та внутрішнім інформаційним загрозам, здібності своєчасно розпізнавати шкідливі впливи, запобігати виникненню та вчасно реагувати на критичні ситуації.

Згідно стандарту ISO/IEC 27001 оцінка інформаційної безпеки повинна проводитись на основі ризик-орієнтовного аналізу, який може бути проведений однією з методик оцінки ризиків, яка враховує технічні, технологічні та організаційні складові ІБ. Однак на даний час майже відсутні інформаційні технології оцінювання рівня інформаційної безпеки, а ті, що є, спрямовані на оцінку ризиків, які враховують різноманіття ресурсів та їх цінність, загрози та вразливості систем, і майже не враховують важливі фактори безпеки внаслідок людино-машинної взаємодії. Це питання визначається напрямком забезпечення культури інформаційної безпеки організації, яка акцентує увагу на визначенні належних організаційних заходів для формування безпечної поведінки користувачів та адміністраторів інформаційної системи організації.

Отже розробка методів, моделей та інформаційної технології оцінювання рівня культури інформаційної безпеки організації є **актуальною** задачею.

Все частіше дослідники та практики в даній галузі вказують на можливості формування культури інформаційної безпеки (КІБ) як одну із можливих стратегій розвитку та підтримки системи безпеки організації. Явище культури довго та ефективно використовується для формування необхідної безпечної поведінки та взаємодій, рівня обізнаності щодо реагування на критичні ситуації та забезпечення безпечної професійної діяльності.

Саме важливість ролей персоналу та менеджменту у системі ІБ організації послужили підставою для даного дослідження. Важливість впливу компетентності людини як користувача внутрішнього інформаційного простору, її обізнаності в галузі ІБ, сприйняття важливості ІБ для успіху організації, з одного боку, а також позиції менеджменту щодо ІБ та зацікавленості у створенні безпечного інформаційного простору організації є тими компонентами, що здатні підсилити наявну СЗІБ або стати її слабкою ланкою.

Тому інтеграція принципів ІБ до повсякденної діяльності співробітників через формування культури інформаційної безпеки є одним з ключових елементів до створення та підтримки СЗІБ організації, захисту її інформаційних ресурсів та бізнес-процесів.

Питанням розробки моделей та методів інформаційних процесів та систем оцінювання рівня безпеки організації присвячені дослідження Adele Da Veiga, Jan H. P. Eloff, Thomas Schlienger, Stephanie Teufel, Johan van Niekerk, Rossouw von Solms, Steven Furnell, Kerry-Lynn Thomson, Kerry-Lynn Thomson, Waldo Rocha Flores, Egil Antonsen, Mathias Ekstedt, Katharina Krombholz, Heidelinde Hobel, Markus Huber, Edgar Weippl, Irene Okere, Mariana Carroll, Areej Alhogail та Abdulrahman Mirza, Paschal A. Ochang, Philip J. Irving, Paulinus O. Ofem. Необхідність впровадження процесів контролю безпечної та відповідальної поведінки співробітників організації або підприємства на кожному ієрархічному рівні стала підставою для досліджень науковців В.В. Бєгуна, В.В. Литвинова, Г.А. Новікова та ін. Результати їх діяльності

втілені в прикладній інформаційній технології оцінки культури безпеки об’єктів критичної інфраструктури – атомних електростанцій. Інформаційну систему оцінювання екологічної безпеки гірничо-добувних підприємств запропоновано І.В. Лесніковою та Н. М. Ястребовою.

У роботах, присвячених оцінці системи забезпечення інформаційної безпеки організацій, увага приділена визначенню ступеня захищеності інформаційної системи організації, в той час як проблемам виявлення рівня персональної ІБ-культури приділяють увагу лише в якості допоміжного елементу СЗІБ організації. Аналіз досліджень показав слабку формалізацію оцінки рівня КІБ як на рівні персоналу, так і організації в цілому, а також відсутність проведення повномасштабної оцінки, що залишає поза увагою основних учасників внутрішнього інформаційного простору організації – її працівників.

Отже, **актуальним науковим завданням** є розроблення моделей та методів інформаційних процесів оцінювання рівня КІБ організації, які дозволять автоматизувати систему визначення поточного рівня КІБ організації з врахуванням персональних показників співробітників, актуальних ІБ-ризиків та нормативних вимог до ведення безпечної діяльності організації в умовах інформатизації. Крім того, не менш важливим є завдання визначення моделі та архітектури інформаційної системи комплексної оцінки культури інформаційної безпеки організації.

Зв’язок роботи з науковими програмами, планами, темами. Представлена дисертаційна робота запланована та виконана в рамках пріоритетного напряму розвитку науки і техніки в Україні «Інформаційні та комунікаційні технології» (Закон України про внесення змін до Закону України про пріоритетні напрями розвитку науки і техніки від 9 вересня 2010 року, № 2519-VI) за пріоритетними тематичними напрямами «Технології та інструментальні засоби електронного урядування. Інформаційно-аналітичні системи, системи підтримки прийняття рішень. Ситуаційні центри» та «Технології та засоби захисту інформації» (відповідно до постанови КМУ

«Про затвердження переліку пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 2020 року» від 07.09.2011 №942); в рамках міжнародного наукового проекту «Cyber Rapid Analysis for Defense Awareness of Real-time Situation – CyRADARS» за грантом NATO SPS, (grant agreement number: G5286)», відповідно до плану науково-дослідних робіт Національного університету «Чернігівська політехніка» «Моделі та методи оцінювання конвергенції систем компетентностей фахівців з використанням технологій штучного інтелекту» (№0120U101929), «Розробка моделей та методів захисту системи від зовнішніх атак з використанням технологій штучного інтелекту» (№0120U101931) та Інституту проблем математичних машин і систем Національної академії наук України «Розвиток базового моделюючого комплексу мережі ситуаційних центрів державних органів сектору безпеки і оборони України в інтересах захисту критичної інфраструктури держави та кібербезпеки» (№0119U000058т).

Мета і завдання дослідження. Метою дослідження є розробка моделей та методів інформаційної технології комплексного оцінювання рівня культури інформаційної безпеки організації з урахуванням особливостей людино-машинної взаємодії, для підтримки прийняття рішень щодо забезпечення відповідного показника безпеки організації.

Досягнення мети передбачає вирішення наступних **задач**:

- Сформувати перелік первинних показників рівня культури інформаційної безпеки організації та її індикаторів.
- Розробити модель інформаційних процесів обчислення рівня культури інформаційної безпеки організації.
- Розробити елементи інформаційної технології визначення рівня культури інформаційної безпеки організації.
- Провести експериментальне дослідження щодо збору та обробки первинної інформації для інформаційної технології оцінювання рівня культури інформаційної безпеки організації.

Об'єкт дослідження – інформаційні процеси визначення культури інформаційної безпеки організації.

Предмет дослідження – методи, моделі та інформаційна технологія комплексної оцінки рівня культури інформаційної безпеки організації з врахуванням особливостей людино-машинної взаємодії.

Методи дослідження. В основу методології дослідження покладено: *принципи системного аналізу та теорії множин*, які використані при аналізі показників культури інформаційної безпеки (КІБ) організації та її працівників, а також при побудові технології оцінювання рівня КІБ організації; *емпіричні методи отримання інформації*, що були застосовані для організації збору первинної інформації шляхом анкетування та подальшої обробки результатів; *методи експертних оцінок,* а саме метод парних порівнянь (ієрархій), котрий був використаний для визначення вагових матриць при створенні моделей для оцінювання рівня персональної КІБ учасників внутрішнього інформаційного простору організації та під час формування моделей ІБ-компетенцій; *метод нечіткої кластеризації* покладений в основу автоматизованого формування анкет, спираючись на особливості професійної діяльності; *метод нечіткого логічного виводу* застосовано для оцінки рівня КІБ як персоналу, так і організації з подальшою рекомендацією стратегії з вдосконалення поточного рівня; *методи м'яких обчислень*, такі як логіка антонімів та нечітка логіка, були використані для оцінки ІБ-компетенцій відповідно до посад, а також загальних обчислень рівня КІБ; *теорія графів* використана для розробки ієрархічної моделі оцінки рівня КІБ організації та моделей ІБ-компетенцій співробітників; *методи об'єктно-орієнтованого аналізу та функціонального моделювання* використані при концептуалізації бізнес-процесів у нотації IDEF0, що покладені в основу створення інформаційної системи оцінювання рівня КІБ організації.

Наукова новизна одержаних результатів:

Вперше:

– розроблена модель інформаційного процесу оцінювання рівня КІБ організації, яка на відміну від існуючих, містить аспекти людино-машинної взаємодії і враховує фактори персональної культури безпеки учасників процесу;
– розроблено метод автоматизованої оцінки рівня КІБ організації, який на відміну від існуючих, базується на використанні нечіткої логіки на основі алгоритму Мамдані, і дозволяє виконувати оцінку поетапно на різних організаційних рівнях.

Дістали подальшого розвитку:

– структура системи ІБ організації за рахунок включення факторів персональної КІБ, що дозволяє враховувати вплив людського чинника на загальну систему безпеки організації;
– метод оцінки рівня персональної КІБ на основі компетентнісного підходу за рахунок використання логіки антонімів, що забезпечує підвищення ефективності проведення таких оцінок.

Практичне значення отриманих результатів. Наведені вище наукові результати у своїй сукупності утворюють нову інформаційну технологію оцінювання рівня культури інформаційної безпеки організації. Запропонована інформаційна технологія може бути корисною для керівників ІБ-підрозділів та організацій для підтримки впроваджених систем забезпечення інформаційної безпеки. Розроблені бізнес-процеси та архітектура можуть бути використані як основа для розроблення власних систем моніторингу культури інформаційної безпеки; модель оцінки персональної культури інформаційної безпеки – при призначенні певних рівнів доступу до інформаційних систем; моніторингу поточного рівня культури інформаційної безпеки персоналу, структурного підрозділу та саме організації для визначення прогалин в обізнаності та компетенцій в галузі ІБ; формуванні команд реагування на інциденти, тощо.

Дана інформаційна технологія має наступне практичне втілення.

Модель нечіткого логічного виводу дає можливість проводити оцінку рівня культури інформаційної безпеки без спеціальних навичок, що значно розширює можливості її використання в неспеціалізованих організаціях.

Забезпечення швидкого самооцінювання виконується за допомогою розробленої автоматизованої телефонної системи (чатботу).

Результати дисертаційного дослідження впроваджені:

- при виконанні міжнародного наукового проекту «Cyber Rapid Analysis for Defense Awareness of Real-time Situation – CyRADARS» за грантом NATO SPS, (grant agreement number: G5286)», науково-дослідних робіт Національного університету «Чернігівська політехніка» «Моделі та методи оцінювання конвергенції систем компетентностей фахівців з використанням технологій штучного інтелекту» (№0120U101929), «Розробка моделей та методів захисту системи від зовнішніх атак з використанням технологій штучного інтелекту» (№0120U101931), а також науково-дослідної роботи «Розвиток базового моделюючого комплексу мережі ситуаційних центрів державних органів сектору безпеки і оборони України в інтересах захисту критичної інфраструктури держави та кібербезпеки» (№0119U000058т) Інституту проблем математичних машин і систем Національної академії наук України;
- на ПАТ «ЧЕЗАРА» під час впровадження тестування персоналу на стадії підбору та приймання на роботу на предмет виявлення базового рівня персональної культури інформаційної безпеки;
- в Державному науково-випробувальному інституті випробувань та сертифікації озброєння та військової техніки при розробці документації інформаційних систем «Інформаційна система з доступом до мережі Internet (ІСД-Internet)» та «Система електронного документообігу (СЕДО)»;
- у навчальному процесі Чернігівського національного технологічного університету (Національного університету «Чернігівська політехніка») при проведенні лекцій та лабораторних робіт з дисципліни «Моделі та

системи штучного інтелекту» – в процесі навчання бакалаврів спеціальності 121 – «Інженерія програмного забезпечення» на кафедрі інформаційних технологій та програмної інженерії.

Особистий внесок здобувача. Наукові результати, викладені в дисертаційній роботі, отримані автором особисто. В наукових роботах, опублікованих у співавторстві, в дисертації використані лише ті ідеї та положення, що є результатом особистої роботи.

Апробація результатів дисертації. Основні положення дисертаційного дослідження доповідалися та обговорювалися на другій всеукраїнській науково-практичній конференції «Перспективні напрями захисту інформації» (м. Одеса, вересень 2016), шістнадцятій науково-технічній конференції "Створення та модернізація озброєння і військової техніки в сучасних умовах" (м. Чернігів, вересень 2016), міжнародній конференції «Проблеми зняття з експлуатації об'єктів ядерної енергетики та відновлення навколишнього середовища» INUDECO (м. Славутич, квітень 2017, квітень 2018, квітень 2020), міжнародній науково-практичній конференції студентів, аспірантів і молодих вчених «Юність науки – 2017: соціально-економічні та гуманітарні аспекти розвитку суспільства» (м. Чернігів, квітень 2017), всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Новітні технології у науковій діяльності і навчальному процесі» (м. Чернігів, квітень 2017), міжнародній науково-практичній конференції «Математичне та імітаційне моделювання систем» (м. Чернігів, червень 2017; с.м.т. Жукін, червень 2018; м. Чернігів, червень 2019, м. Чернігів, червень 2020), п'ятій міжнародній науково-практичній конференції «Інформаційні технології та взаємодії» (м. Київ, листопад 2018), міжнародній науково-практичній конференції «Advances in Computer Science for Engineering and Education II. ICCSEEA» (м. Київ, січень 2019), всеукраїнській науково-практичній конференції «Безпека соціально-економічних процесів в кіберпросторі» (м. Київ, березень 2019), шістнадцятій міжнародній конференції «Управління проектами у розвитку суспільства» (м. Київ, травень 2019).

Публікації. За темою дисертаційного дослідження з викладенням основних результатів опубліковано 18 наукових праць. Серед них 5 статей у фахових журналах, 4 з них включені до міжнародної наукометричної бази Scopus [1–3, 5], з яких 3 у закордонних виданнях [2, 3, 5]; 13 праць апробаційного характеру [6-18]. Результати роботи доповідалися на 10 міжнародних наукових конференціях.

Структура та обсяг роботи. Дисертаційна робота складається зі вступу, 4 розділів (глав), висновків, переліку умовних скорочень, переліку посилань зі 122 джерел та 5 додатків. Загальний обсяг роботи становить 194 сторінки, з яких зміст на 3 сторінках, вступ на 9 сторінках, перелік умовних скорочень на 1 сторінці, основний текст на 173 сторінках, список використаних джерел із 122 найменувань на 19 сторінках, 5 додатків на 21 сторінці. Робота містить 67 рисунків (з них 1 рисунок на 1 окремій сторінці) та 8 таблиць (з них 4 таблиці на 14 окремих сторінках).

РОЗДІЛ 1
ХАРАКТЕРИСТИКА МЕТОДІВ ВИЗНАЧЕННЯ РІВНЯ КУЛЬТУРИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ ТА ЇХ КОМП'ЮТЕРНА ПІДТРИМКА

1.1 Загальна характеристика систем інформаційної безпеки організації

Сьогодні ми спостерігаємо за стрімким розвитком технологій, їх невпинне проникнення у кожну сферу людської діяльності. Успіх найвідоміших компаній зумовлений саме провідною діяльністю в галузі новітніх технологій, а інформація поступово трансформувалася з інструменту виробництва на готовий продукт. Так, наприклад, відомості про вподобання користувача або історія його замовлень через Інтернет стала товаром, за який рекламні компанії готові виплачувати непомірні кошти. Інформація має ціну.

Поняття «інформація» є загальнонауковою категорією, виступає як в якості самого продукту, так і в ролі інструменту забезпечення його виробництва. Перехід інформації в категорію цінного ресурсу неминуче призвів до виникнення необхідності цей ресурс захищати. Оскільки сучасні технології та масиви знань ґрунтуються на багатомільйонних інвестиціях, а також являються основою сучасного суспільства і використовуються в кожній сфері людської діяльності, інформація стала об'єктом зацікавленості з боку конкурентів, кримінальних структур, потенційною мішенню для реалізації терористичних актів (блокування або знищення критично важливих систем – медичних, урядових, енергетичних і транспортних, стратегічно важливих об'єктів).

Розуміння важливості інформації як стратегічного ресурсу відобразилося в ряді нормативно-правових актів міжнародного значення та законодавства України, відбулося переміщення на передній план невідкладних проблем інформаційної безпеки в якості одного з ключових компонентів

безпеки національної. Зміна сприйняття інформації спричинила перехід даного об'єкта з категорії «інструмент» в «кінцевий продукт», а питання, що виникли в результаті цих змін, і пов’язані з захистом інтелектуальної власності, сприяли створенню та подальшому розвитку інформаційної безпеки.

Глобальність проблеми інформаційної безпеки підтверджена резолюцією про «Створення глобальної культури кібербезпеки» засідання Генеральної Асамблеї ООН від 31 січня 2003 року [1], що стала основою для посиленого вивчення та дослідження ролі кібернетичної (а також і інформаційної) безпеки як одного з основоположних факторів захисту інформації. Також підкреслено вплив підтримки суспільства в якості одного з визначальних факторів, що обумовлюють ефективність кібернетичної безпеки на міжнародному та національному рівні.

Ставлення до інформації та інформаційної безпеки в Україні регламентується Законом України «Про інформацію» від 02.10.1992 року зі змінами [2], указами Президента України про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України" [3], рішеннями Ради національної безпеки і оборони України від 2 вересня 2015 року "Про нову редакцію Воєнної доктрини України" [4] та "Про Стратегію кібербезпеки України" № 96/2016 від 27 січня 2016 року [5], Законом України «Про національну безпеку України» від 21 червня 2018 року № 2469-VIII [6].

Закон України «Про інформацію» від 02.10.1992 року вкладає в поняття «інформація» наступне визначення [2]: «Інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді».

За наведеними законодавчими документами інформаційна безпека визначається як стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через:

неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [7].

Проблеми захисту інформації завжди були невід'ємною частиною бізнес-рутини підприємств та організацій. Власні розробки, клієнтські бази, плани з випуску, автоматизовані лінії – кожен з цих об'єктів є мішенню для конкурентів. Різноманіття шляхів реалізації атак з метою заволодіння або знищення критичних ресурсів (якою сьогодні виступає інформація) спонукає до пошуку ефективних заходів протидії.

Інформація, що визначається організацією як цінна, з позиції інформаційної безпеки повинна володіти наступними необхідними властивостями [8]:

"*Конфіденційність* – властивість (характеристика) інформації, що вказує на необхідність обмеження кола суб'єктів, які мають доступ до даної інформації".

"*Цілісність інформації* – властивість інформації існувати в невикривленому вигляді (незмінному по відношенню до деякого фіксованого для неї стану)".

"*Доступність* – стан інформації (ресурсів ІС), при якому суб'єкти, які мають права доступу, можуть реалізовувати їх безперешкодно".

Основні визначення терміну «інформаційна безпека» наведені в таблиці 1.1.

Таблиця 1.1 – Порівняльний аналіз визначень ІБ

Автор(и)	Визначення ІБ	Суб'єкт
В.А. Ліпкан	"Складова національної безпеки, процес управління загрозами та небезпеками державними і недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України;	Держава, людина

Продовження Таблиці 1.1

Автор(и)	Визначення ІБ	Суб’єкт
	вдосконалення державного регулювання розвитку інформаційної сфери, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; активне залучення засобів масової інформації до боротьби з корупцією, зловживанням службовим становищем, іншими явищами, які загрожують національній безпеці України; неухильне дотримання конституційного права громадян на свободу слова доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції; вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України" [9].	
А.В. Велігура	"Комплекс заходів та засобів щодо забезпечення збереження інформації, що знаходиться в системі інформаційного забезпечення діяльності підприємства, переданої, оброблюваної, а також тієї, що зберігається та надається системою" [10].	Інформація
А.А. Кобозєва та ін., О.О. Шумейко	"Захищеність інформації, ресурсів і підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати неприйнятного збитку суб'єктам інформаційних відносин – виробникам, власникам і користувачам інформації і підтримуючої інфраструктури" [11, 12].	Інформація, ІР
Ю.М. Загинайлов	"З позиції управління інформаційною безпекою організації ІБ визначається, як властивість інформації зберігати конфіденційність, цілісність та доступність, а власне ІБ організації – стан захищеності об’єктів (активів) організації, за якого забезпечується	Інформація

Продовження Таблиці 1.1

Автор(и)	Визначення ІБ	Суб’єкт
	конфіденційність, цілісність, доступність інформації" [8].	
	"З позиції безпеки системи інформаційних технологій, на яких засновані бізнес-процеси організації, ІБ – це всі аспекти, що пов’язані з визначенням, досягненням та підтримкою конфіденційності, цілісності, доступності, безвідмовності, підзвітності, автентичності та достовірності інформації або засобів її обробки" [8].	Властивості інформації
Г.А. Атаманов	"Ситуація, при якій йому (суб'єктові) забезпечено фізичний та семантичний доступ до інформації в обсязі та якості, необхідних для прийняття вірних рішень, а також йому не наноситься шкода шляхом впливу на його інформаційну інфраструктуру, його інформаційну функцію та вагомі для нього інформаційні ресурси, внаслідок чого він зберігає здатність та можливість ставити позитивні соціально вагомі цілі, спрямовані на прогресивний розвиток власний та соціуму, забезпечувати умови та зберігати можливості їх досягнення" [13].	Людина, корпорація (формальна або неформальна) або держава

Порівняння визначень свідчить, що на даний час немає узгодженої думки щодо суб’єкту інформаційної безпеки та його критичних властивостей. З одного боку, ІБ покликана захищати інтереси індивідів (стейкхолдерів), з іншого – це стан інформаційного простору.

Згідно [13] інформаційна безпека суб'єкта досягається завдяки:

- забезпеченню суб’єкта достовірною, достатньою та своєчасною інформацією для прийняття правильного рішення;
- виключенню або зменшенню ймовірності реалізації деструктивних наслідків на інформаційну інфраструктуру та інформаційну функцію суб’єкта;
- захисту суттєвих для суб’єкта ІР від знищення, викривлення/спотворення, блокування або розкриття (збереження

властивостей ІР: цілісності, доступності, достовірності, захисту від некоректної зміни статусу).

Складну систему взаємозв'язків між елементами комп'ютерної мережі, інформаційними ресурсами, а також ІБ та кібербезпекою в інформаційному просторі організації приведено в ISO/IEC 27032 [14] (рисунок 1.1).

Рисунок 1.1 – Логічні взаємозв'язки між інформаційною безпекою та кібербезпекою організації [14]

Також в ISO/IEC 27032 зазначено необхідність безперервного вдосконалення СІБ організації через вплив СМІБ, що створена в рамках комплексної СЗІБ (рисунок 1.2).

Рисунок 1.2 – Взаємозв'язок СІБ, СМІБ та СЗІБ [15]

У звіті [16] зазначено, що деякі компанії схильні недбало ставитися до захисту, оскільки недостатньо переконані в тому, що можуть зацікавити зловмисників через відсутність привабливих ресурсів. Однак, навіть не приймаючи до уваги можливість втрати інтелектуальної власності або персональних даних клієнтів, компанія може представляти цінність як посередник в ланцюзі компрометації своїх контрагентів.

Залежно від зрілості ІБ-процесів, що супроводжують діяльність організації, вирізняють п’ять етапів розвитку СІБ організації [8, 10]. Про це свідчать принципи накопичення та обробки інформації, її захисту, документування процесів, розподіл відповідальності між співробітниками, тощо.

Подібна модель зрілості відображена в [17]. Ступінь стабільності ІБ-процесів розглядається за п’ятьма критеріями: ідентифікація, захист, виявлення, реагування, відновлення.

Рисунок 1.3 – Модель зрілості СЗІБ організації [17]

В роботі Ю.М. Загинайлова [8] приведений докладний опис етапів зрілості процесів та корпоративної культури організації, а також становлення та розвиток СЗІБ. Короткий зміст наведено в таблиці 1.2.

Таблиця 1.2 – Рівні зрілості організації в сфері захисту інформації та їх характеристики [8]

Рівень зрілості		Характеристики		
№	Назва	Засоби захисту	Персонал, відповідальний за захист	Регламентація
1	Хаос (спонтанні інформаційні зв'язки)	Відсутні	Відсутній	Відсутні
2	Фрагментарний захист	Використовуються частково	Призначені відповідальні за захист	Наявні окремі документи, що регламентують захист
3	Системний захист	Використовуються поєднані в систему засоби захисту	Сформована служба захисту інформації	Діяльність щодо захисту регламентована нормативними документами
4	Керований захист	Функціонує комплексна система захисту інформації на підприємстві	Відповідальний за захист інформації персонал має спеціальну підготовку (освіту, перекваліфікацію)	Запроваджена система управління ІБ організації на основі ISO 27001 та ISO 27002
5	Управління якістю ІБ (оптимізований)	Функціонує комплексна система захисту інформації на підприємстві	Відповідальний за захист інформації персонал має спеціальну підготовку (освіту, перекваліфікацію)	Запроваджені: СЗІБ на основі ISO 27001 та ISO 27002; система менедж-менту якості ІБ на основі ISO 27001

Як бачимо, відповідальне ставлення до проблем інформаційної безпеки організації та прийняття рішення про необхідність впровадження системи захисту власних інформаційних активів характерна для більш високих рівнів зрілості. За таких умов спостерігається гармонійна інтеграція КІБ до корпоративної (організаційної) культури компанії.

1.2 Роль та місце культури інформаційної безпеки в сучасних організаціях

Розвиток мережного суспільства та повсюдне поширення інформаційних технологій призвели до фундаментальних перетворень, що відкрили нові можливості для досягнення успіхів у бізнесі, виробництві високотехнологічних товарів, соціальної взаємодії [18]. Тим не менш, з новими можливостями з'явилися (або проявилися) і нові загрози, що пов'язані із «цифровим всесвітом» Всеосяжного Інтернету [19].

При цьому все більшого значення набуває питання зростання ролі КІБ користувача інформаційної системи як ключового чинника зниження впливу людського чинника на загальну безпеку.

Для учасників інформаційних процесів в організації високонадійна КІБ передбачає добре знання її суті та її ворогів, впровадження рішень щодо захисту даних на всіх рівнях, навчання персоналу, вживання заходів, які спонукають співробітників розпізнавати проблеми в цій галузі та своєчасно на них реагувати, а також об'єднання колективу завдяки спільним переконанням щодо необхідності впровадження захисту інформаційних активів та розуміння потенційних наслідків компрометації наявної системи захисту [20-21].

Однією з ключових проблем при розробці та впровадженні СЗІБ стає визначення поточного стану КІБ співробітників та учасників інформаційних процесів організації. Вимогам щодо технічного аспекту ІБ присвячено багато галузевих стандартів, рекомендацій та методик, що призначені для обґрунтування, оцінки та вдосконалення системи політик та засобів забезпечення ІБ. Стосовно найбільш вразливого елемента даної системи – людини, – у цьому питанні, традиційно, відповідальність покладена на співробітників ІТ-підрозділу та часто розглядається як задача, що вирішується за рахунок технічної та організаційної складових СЗІБ.

Свій внесок у послаблення СЗІБ організації робить і політика BYOD, що дозволяє використання власних гаджетів. З одного боку, це дозволяє

зменшити витрати на придбання обчислювальної техніки, надаючи змогу співробітникам використовувати те обладнання, яке задовольняє його виробничі потреби за обчислювальною потужністю. З іншого боку, такий підхід вимагає розроблення певних заходів контролю та підтримки належного ІБ-захисту.

Проте проблема інформаційних впливів не є новою, та її поширення в мережах добре вивчено. Крім того, варті уваги такі людино-орієнтовані загрози, як підроблені листи та посилання, фальшиві профілі у соціальних мережах, хибні поради або допомога (технічна, медична, юридична тощо), яку люди використовують для пошуку потрібної інформації, навчання, бізнесу або роботи. І такі природні риси як необачність та довірливість легко можуть завдати шкоди не лише користувачеві, а й пов’язаним із ним інформаційним ресурсам, до яких людина має доступ в рамках професійної діяльності. В решті решт, людина може бути використана як посередник для здійснення несанкціонованого доступу до ресурсів компанії.

Останнім часом людина стала об'єктом інформаційних впливів, тож для зменшення наслідків необхідний системний підхід. Він повинен містити елементи різних технічних, економічних, філософських, соціологічних та економічних сучасних розробок. Важливо розуміти не лише технічні аспекти побудови комп’ютерних мереж, але й здатність моделювати реакцію та прийняття рішення людиною в результаті інформаційних впливів з метою створення ефективних інформаційних систем захисту та запобігання атакам. Сьогодні для вирішення цих питань активно застосовуються експертні системи та системи на основі нейронних мереж, що використовують різні алгоритми побудови баз знань у системах технічної інформаційної безпеки.

У сучасному світі здійснюється постійний моніторинг інформації в комп'ютерних мережах. Для пошуку та збору інформації використовуються спеціальні системи збору даних – так звані "роботи" або "павуки". Принцип функціонування такого робота полягає у перетині набору веб-посилань за заздалегідь визначеним графіком та збором зі сторінок необхідної інформації.

При цьому він застосовує широкий спектр засобів мовного, семантичного та статистичного аналізу. Такі системи автоматично перехоплюють будь-яку інформацію, яка відстежується, як тільки вона з’являється у видимій мережі. Автоматизований видобуток інформації стає у нагоді для спамерів, а соціальні мережі – невичерпним ресурсом для отримання особистої інформації користувачів з подальшим її використанням для створення підроблених аккаунтів в інших соціальних мережах. Одним із засобів протидії цьому видові загроз є пильне ставлення до інформації, що розміщується у вільному доступі.

У сучасній ситуації одними з рушійних сил успішної бізнес-діяльності виступають технології, мобільність та доступність послуг. Інвестиції в інформаційні активи оцінюються нарівні з матеріальним капіталом, і захист цих інформаційних активів заслуговує на посилену увагу. Незважаючи на інтенсивний розвиток технічних засобів захисту інформації, на які власники та особи, відповідальні за інформаційні активи, покладаються в більшості випадків, працівники все ще залишаються не останнім фактором, що впливає на безпеку та цілісність інформаційних активів організації. Захищеність ресурсів, обчислювальної потужності, програмного забезпечення та кінцевих користувачів все ще залежить від здатності персоналу протистояти зовнішнім та внутрішнім інформаційним загрозам, здатності своєчасно розпізнавати та запобігати виникненню та реагувати на критичні ситуації.

У зв'язку з цим науковці та фахівці з питань ІБ регулярно вказують на необхідність впливу на ІБ організацій через формування адекватного рівня культури інформаційної безпеки (КІБ). Явище культури довго та ефективно використовується для формування необхідної безпечної поведінки та взаємодій, рівня обізнаності щодо дій у критичних випадках та забезпечення безпечної трудової діяльності [22].

Дослідження проблем формування необхідного рівня КІБ для працівників організації справедливо присутні серед робіт, присвячених захисту інформаційних активів та безпеці комп'ютерних мереж.

Johan van Niekerk та Rossouw von Solms [23] наголошують на важливості впровадження КІБ співробітників в якості субкультури в рамках організації для управління впливом людського чинника на інформаційну безпеку організації. Раніше в роботі Нго (Ngo) та ін. [24] було зазначено невід'ємність КІБ від корпоративної культури.

На необхідність визначення рівня КІБ організації з метою подальшої розробки заходів для покращення поточної ситуації вказують Steven Furnell та Kerry-Lynn Thomson [25]. Згадане дослідження розглядає можливість інтеграції КІБ до природної поведінки працівників.

В результаті інтенсивної дослідницької діяльності Adele Da Veiga et al. було представлено ряд робіт, присвячених впливу людського чинника на систему менеджменту інформаційною безпекою. Зокрема, у роботі [26] зазначається вплив КІБ працівників на зменшення ІБ-ризиків, пов'язаних із взаємодією працівників та активів.

Все частіше дослідження КІБ враховують такі фактори, як національні культура та менталітет. Прикладом виступає дослідження Waldo Rocha Flores, Egil Antonsen та Mathias Ekstedt [27], що вказує на вплив вищезазначених факторів на діяльність організацій у глобальному середовищі.

Цей огляд не буде повним без згадки імен Thomas Schlienger та Stephanie Teufel, робота яких [28] стала відправною точкою для багатьох дослідників та керівництвом до дій для менеджерів компаній, зацікавлених у подальшому посиленні захисту IP шляхом залучення працівників.

Враховуючи можливі перепони під час прищеплення та розвитку КІБ співробітників, з якими можуть зіткнутися керівники (наприклад, страх, опір та розгубленість), Areej Alhogail та Abdulrahman Mirza запропонували ефективні моделі управління змінами та багатоступінчасті фрейми, що описані в [29].

Крім того, велику та трудомістку роботу з аналізу та систематизації досліджень у галузі КІБ організацій провели Emad Sherif, Steven Furnell та Nathan Clarke, та представили у роботі [30].

Вищезазначені роботи є лише невеликою частиною сучасних досліджень, заснованих на глибокому розумінні людської психології, соціальних взаємодій, управлінні персоналом, інформаційної та мережевої безпеки та корпоративної культури. Нові інформаційні технології з'являються та розвиваються щодня, і інформаційна безпека, очікувано, постає перед новими викликами.

Однак питання автоматизації управління КІБ ще недостатньо вивчене. Не існує комплексних програмних засобів, що дозволяють оцінити, спланувати та контролювати зміни в КІБ організації. Такі засоби повинні враховувати технічні та особисті компоненти КІБ, а також ступінь ризику на різних рівнях організації комп'ютерних мереж.

Така пильна увага до проблеми ІБ викликана неминучим зростанням підстав – кількість інцидентів ІБ зростає, як це чітко видно з рисунку 1.4. Наведені цифри, запозичені у звітах Risk Based Security Group за 2012–2018 р. [31-40], свідчать про це.

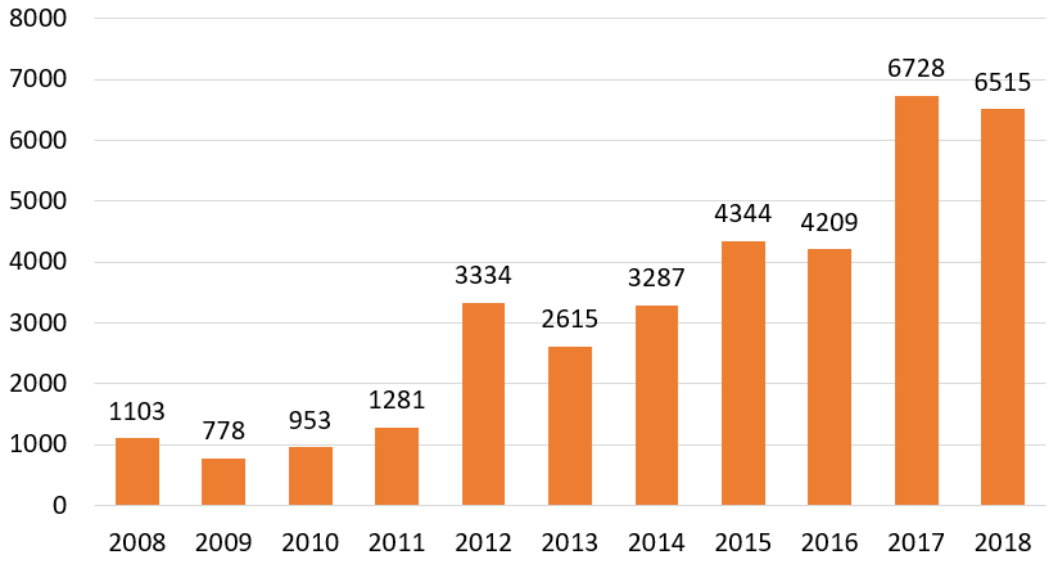

Рисунок 1.4 – Динаміка ІБ-інцидентів у 2008-2018 р.р.

За даними звітів, місце лідера серед інцидентів за типом порушень (Incidents by Breach Type) закономірно належить хакінгу. У той же час, набирають популярність атаки на базі фішингу, web стабільно присутній серед ІБ-інцидентів (рисунок 1.5). Зі зростаючими темпами розвитку електронних

технологій та тенденцією до мінімізації розмірів електронної апаратури, скімери стали настільки ж поширеним явищем, як і безготівкові платежі банківськими картками. Вірусна активність в 2016-2017 роках проявилася в діяльності вірусів-шифрувальників WannaCry, Petya-A, GandCrab, банківських троянів Zeus, Ursnif тощо.

Шахрайство та напади з використанням методів СІ залишаються широко розповсюдженими. Незважаючи на те, що цей тип ІБ-інцидентів не був включений до топ-5 подій за 2017 рік, шахрайство та СІ послідовно займають 7-8 місце у Топ-10 звітів за 1-й квартал за 2017 рік [36-38]. Її прояв у 2018 році не дозволяє ігнорувати або нехтувати цим видом загроз.

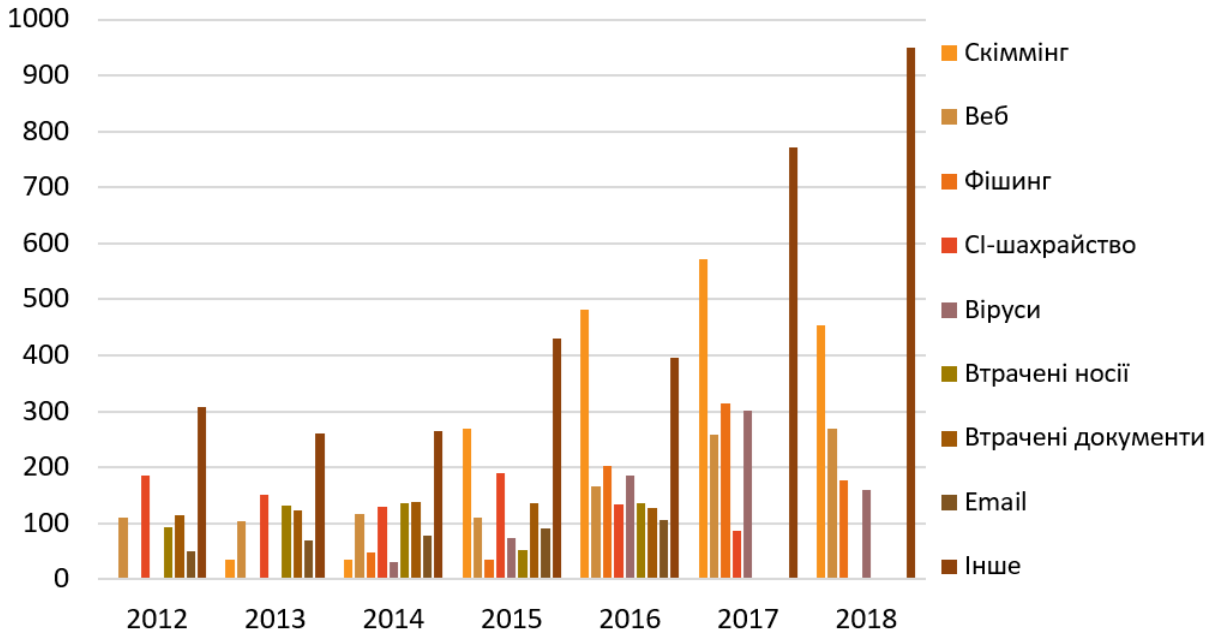

Рисунок 1.5 – Інциденти за типом порушень

Переважна більшість жертв ІБ-інцидентів – це бізнес, підприємства, організації та виробництво. Аналіз статистики інцидентів очікувано демонструє зловмисну активність ззовні. У той же час, розподіл внутрішніх джерел ІБ-інцидентів свідчить про те, що більшість інцидентів трапляються через випадковість та необережність, хоча вони конкурують із частотою шкідливих дій, що відбуваються всередині організацій (рисунок 1.6).

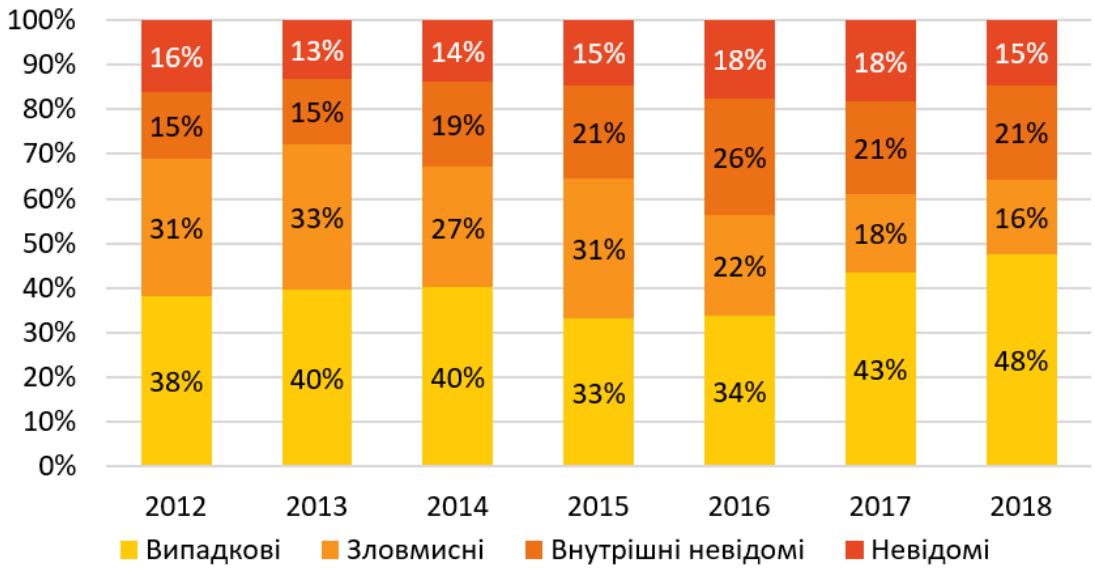

Рисунок 1.6 – Інциденти внутрішнього походження

Якщо з дією інсайдерів та мстивих і незадоволених співробітників прийнято боротися з використанням DLP[1]-систем, то на допомогу в боротьбі з випадковими явищами знов приходить один з найсильніших проявів та інструментів у формуванні та управлінні безпечною поведінкою і переконаннями – феномен культури. І зокрема – культури інформаційної безпеки.

Katharina Krombholz та ін. [41] підкреслили, що соціальні мережі містять безліч особистої інформації, яка може бути використана як початкове джерело для атак на базі CI.

Наявність активного та постійно оновлюваного профілю в одній із популярних соціальних мереж реалізує ряд можливостей:

– автоматизований видобуток особистої інформації користувачів соціальних мереж;
– встановлення переконливого підробленого профілю користувача в іншій популярній соціальній мережі та взаємодія з іншими довіреними користувачами (друзями);

[1] Data Leak Prevention System – система запобігання витоку даних

– створення сприятливих умов для соціального фішингу та контекстно-спрямованого спаму.

Зараз майже кожна сучасна компанія має офіційний профіль у Facebook та власний веб-сайт. Основними елементами є опис послуг або продуктів, інформація про менеджерів або продавців (імена, прізвища та посади), а також канали для зв'язку (гаряча лінія, електронна та фізична пошти, месенджери та інші комунікації). Для досвідченого соціального інженера соціальні мережі пропонують необмежене джерело інформації, яке залюбки наповнюють самі власники.

Katharina Krombholz та ін. [41] також зауважили, що мобільні додатки стали частіше використовуватися в якості каналу для здійснення атак методом CI. Для ділового спілкування, особливо мобільного обміну повідомленнями та додатків електронної пошти, які використовуються для обміну інформацією персоналом, політика BYOD дозволяє і навіть заохочує співробітників використовувати персональні мобільні телефони та планшети, які є дуже вразливими через додатки, що можуть призвести до реалізації CI-атак та до збору конфіденційної інформації. Особливо, коли зловмисник є програмним розробником.

Можливість використання культури як носія та поширення безпечної та усвідомленої поведінки розглядається у багатьох потенційно небезпечних галузях знань, таких як ядерна енергетика, екологія, медицина, – у сферах, де діяльність людини може мати руйнівні наслідки. Наприклад, культура розглядається як джерело багатства та раритетних факторів при моделюванні економічної поведінки [42].

Проблеми оцінки культури в різних галузях хвилювали багатьох вчених. Культуру як чинник забезпечення екологічної безпеки досліджували І.В. Леснікова та Н. М. Ястребова. Питанням формування культури безпеки в галузі ядерної енергетики присвячені роботи В.В. Бєгуна, В.В. Литвинова, Г.А. Новікова та ін.

Роботи T. Schlienger, S. Teufel [43] присвячені розгляду КІБ з позицій впливового інструменту існуючої корпоративної культури. Більш детально аспекти КІБ організації, що безпосередньо пов'язані з джерелом ризику – персоналом, представлені у роботах K. Krombholz та ін. [41], F. Mouton та ін. [44], I. Okere та J. van Niekerk, M. Carroll [45], A. Alhogail та A. Mirza [46], Paschal A. Ochang та ін. [47]. Така пильна увага до людського чинника обумовлена неможливістю виключити людину як учасника процесу обробки інформації. І, як наслідок, наявні прогалини в КІБ прямих виконавців стануть джерелами ІБ-загроз для організації.

Ефективними моделями оцінки рівня культури в цілому та культури інформаційної безпеки, зокрема, визнаються моделі показників, розглянутих у [48], а також представлені в моделях прихованих змінних, визначених причинно-наслідковими та ефект-показниками [49].

У соціології вплив на поведінку людини для забезпечення виробничого процесу визначається як формування соціально-технологічної культури. За визначенням [50], "соціально-технологічна культура працівників – це органічна частина корпоративної культури, спрямована на інтеграцію досягнень технічних та гуманітарних наук, застосування інтегрованих принципів до вивчення соціального простору компанії, її «здорового» функціонування на конкурентному ринку та його активного розвитку відповідно до цілей розвитку організації".

Згідно з твердженням [46], КІБ можна визначити як сукупність сприйняття, позицій, цінностей, припущень та знань, які керують взаємодією людини з інформаційними активами організації з метою впливу на поведінку працівників щодо збереження інформаційної безпеки. Також можна відзначити одне з концептуальних визначень КІБ, яке відображає ставлення до інформації та інформаційного простору як до одного з найнебезпечніших та найвпливовіших середовищ. Таким чином, зразкове ставлення до культури безпеки сформувалося в атомній енергетиці: "Культура безпеки – це такий набір характеристик і особливостей діяльності організацій та поведінки

окремих осіб, який встановлює, що проблемам безпеки атомних станцій, як таким, що мають вищий пріоритет, приділяється увага, яка визначається їх значущістю" [49].

Вищенаведене визначення охоплює не лише апаратні та технологічні проблеми інформаційних ресурсів, а й сукупність шаблонів поведінки, якими керується персонал (оператори, адміністратори, інші працівники організації, управління) в процесі внутрішньої та зовнішньої діяльності. Важливість постійного дотримання принципів ІБ обумовлена масштабом та безперервністю інформаційних загроз, багатовекторністю атак на інформаційні ресурси, складним розумінням прихованої цінності інформації, яка сприймається як не важлива тощо.

Отже, культура інформаційної безпеки – це комплексна характеристика інформаційної безпеки організації, що відображає організацію технологічних процесів та стан підготовки персоналу, які відповідають припустимим ризикам.

Для того щоб визначити ситуацію стосовно формування культури ІБ на рівні організації, слід розглянути модель культури ІБ [51-53], яка є невід'ємною складовою організаційної культури: *поверхневий рівень* – артефактів та створень, визначається як видимий, але ще не інтерпретований, – фізичний вплив на формування культури ІБ співробітників за допомогою проведення навчання та контролю рівня компетенцій; *середній рівень* – колективних цінностей, норм та компетенцій, що є частково помітним та свідомим, – збереження рівня КІБ організації за рахунок постійного інформування співробітників з питань ІБ для підвищення безпеки організації в усіх її проявах; *глибинний рівень* – основних припущень та переконань, що є неусвідомленим та прихованим – усвідомлення, що кожен працівник є носієм КІБ, а тому і учасником організаційної культури загалом (рисунок 1.7).

Рисунок 1.7 – Модель КІБ організації за Е.Шейном

Управління КІБ, як і організаційною культурою в цілому, можливе лише при ретельному, глибокому та тривалому процесі напрацювання, оцінювання та комплексного застосування позитивних управлінських рішень. Формування ефективної корпоративної культури – процес складний та тривалий, потребує критичного оцінювання та постійного вдосконалення. Не менш складний та тернистий шлях формування та вдосконалення КІБ, оскільки впровадження жорсткішої ІБ-політики організації спричинить супротив та непорозуміння з боку персоналу, а також певну інертність власне організації як багатокомпонентної системи.

Adéle da Veiga та Nico Martins [54] застосовують поняття субкультури. Базовим твердженням є те, що диференціація субкультур зумовлюється відмінностями між групами людей. З цієї позиції КІБ організації розглядають як домінуючу над груповими субкультурами. Поняття групової субкультури, на наш погляд, є правомірним еквівалентом КІБ підрозділу, що зумовлене виконанням суміжних посадових обов’язків, спільним емоційним кліматом, спілкуванням тощо.

Рисунок 1.8 є адаптацією моделі, запропонованої Don Hellriegel та співавторами, а також баченням Adéle da Veiga та Nico Martins з врахуванням наявності субкультур у загальній КІБ організації, проте з інтерпретацією субкультур як КІБ структурних підрозділів (СП).

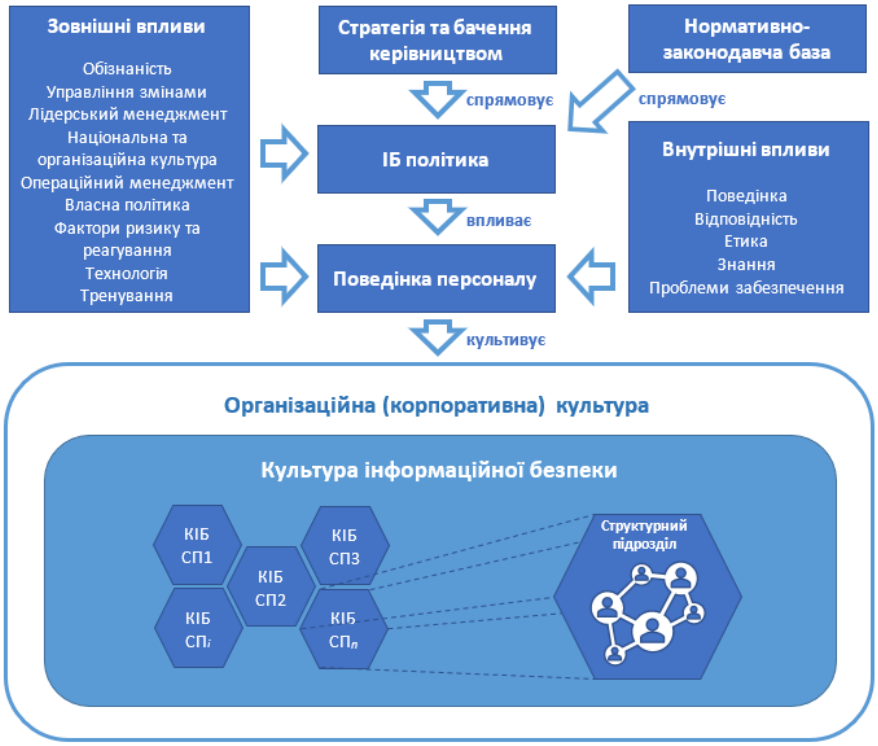

Рисунок 1.8 – Формування КІБ організації

Формування КІБ відбувається під впливом ряду зовнішніх та внутрішніх чинників. Так, КІБ організації створюється, проходить певні етапи розвитку та відображає зміни у зовнішньому середовищі та внутрішньому інформаційному просторі організації. Можна провести аналогію: виникнення, розвиток та закріплення КІБ подібне до формування набутого рефлексу на подразник. Тож КІБ організації є реакцією на вплив динамічних чинників з метою уникнути збитків від ІБ-загроз.

Таким чином КІБ організації можна описати як коваріацію факторів, оцінка пливу яких може бути визначена на основі непараметричного аналізу.

Збиток, нанесений компаніям в результаті реалізації кібератак, щорічно і неухильно зростає. Суттєвим ускладненням є проведення оцінки вартості наявних інформаційних ресурсів. Оскільки інформація виступає в ролі

сировини і в той же час результатом виробництва – кінцевим продуктом, на кожному з етапів інформація стає активами організації. В якості інформаційного активу можуть виступати план випуску продукції, передові розробки, які очікують завершення процедури патентування, облікові дані банківських клієнтів, персональні дані громадян, які зберігаються в інформаційних системах державних органів. Втрата такого активу в результаті реалізації атаки на корпоративну інформаційну мережу може привести до фінансових, соціальних, юридичних та навіть екологічних наслідків.

Збиток, що завдають віруси, може бути невідчутним і незначним, якщо це невисокий приріст трафіку через приховану розсилку спаму або зниження продуктивності зараженого комп'ютера. Інша справа, якщо мова йде про несанкціоновані дії, спрямовані на знищення інформаційної мережі, компрометацію системи криптозахисту, отримання віддаленого доступу до ресурсів, захоплення комерційної інформації та диверсій у вигляді знищення цінних розробок або каналів комунікацій.

Особливо гостро постає проблема формування спільної КІБ учасників при здійсненні проектної діяльності. Різні групи учасників, що є представниками різних груп (культурних, соціальних, національних, релігійних тощо), мають різнорідні набори цінностей та мотивів [55]. Залежно від етапу проекту рівень зацікавленості у підтримці належного рівня КІБ також може коливатися.

Стандарт ISO/IEC 27001:2015 вимагає поширення дії СМІБ і на корпоративну рутину, і на зовнішню проектну діяльність організації. Тож впровадження спільної КІБ для географічно розподілених команд-учасників міжнародних проектів гармонійно інтегрується до PMBoK-методології [56].

Думки фахівців щодо матеріальності або нематеріальності інформаційних активів поділяються (наприклад, [57] проти [58]), так само як і уявлення про ціну і цінність інформації. Багато дослідників і аналітиків акцентують увагу на ціні IP, яка виражається в грошовому еквіваленті. Примітною також є позиція [57], що протиставить наведеним вище факторам

– ціна (динамічна характеристика) і цінність (суб'єктивна характеристика), – зростаючу роль навичок та вмінь працювати з інформацією, використовувати її у власних інтересах.

Так, згідно [58], оцінювання ІР пов'язане із рядом проблем. На першому етапі – їх формуванні в якості об'єкта – виділення із загального масиву даних саме цінних ІР здійснюється завдяки оцінюванню керівниками та експертами – вузькоспеціалізованими фахівцями в даній області. На другому етапі – визначенні цінності ІР в загальноприйнятому і зрозумілому еквіваленті – грошовому. Оскільки завдання оцінки ІР слабо формалізується, а також з огляду на суб'єктивність при формуванні ціни ІР, точно визначити вартість ІР неможливо. Також завдання ускладняється, якщо взяти до уваги той факт, що інформаційні активи є динамічною структурою з вкрай невизначеним терміном корисної експлуатації через швидку втрату актуальності [58].

Як зазначено в [59], цінність інформаційних активів визначається величиною прямого або непрямого збитку, що завдається бізнесу в результаті інцидентів безпеки, пов'язаних з розкриттям, несанкціонованою модифікацією, тимчасовою недоступністю або руйнуванням активів. Наслідками таких інцидентів можуть бути втрачені вигоди, позбавлення конкурентних переваг, погіршення іміджу організації, заподіяння шкоди інтересам третьої сторони, штрафи, прямі фінансові збитки або дезорганізація діяльності. Для кожного активу слід розглядати найгірший сценарій розвитку подій.

Для оцінки можливого збитку в результаті здійснення загроз щодо активів можуть використовуватися такі критерії:

- збитки комерційним інтересам партнерів та третіх осіб;
- санкції з боку правоохоронних і регулюючих органів (штрафи, адміністративна та кримінальна відповідальність);
- збитки комерційним інтересам організації;
- фінансові втрати;
- збиток репутації організації;

– дезорганізація діяльності, погіршення морального клімату в колективі, зниження ефективності роботи.

У загальному вигляді захисна стратегія реагування на інциденти виглядає наступним чином (Рисунок 1.9):

Рисунок 1.9 – Фази реагування на інцидент [60]

Ефективність кожного з наведених етапів в певній мірі залежить від швидкості реакції персоналу, вміння виявити нестандартну поведінку системи або мережі, здатності ліквідувати наслідки, а також вміти аналізувати причини, що призвели до появи інциденту, та засвоювати уроки.

1.3 Аналіз методів оцінки рівня культури інформаційної безпеки організації та їх програмне забезпечення

Сьогодні склалася така ситуація, за якої оцінка рівня культури безпеки (КБ) (загальної безпеки, як комплексної системи) сформована лише у такій критичній галузі як ядерна енергетика. Рівень КБ на АЕС є головним показником безпеки експлуатації таких підприємств, оскільки наслідки навіть, здавалося б, незначних порушень можуть бути катастрофічними.

Так, наприклад, основними методиками оцінки рівня КБ на підприємствах атомної енергетики є:

– керівництво ASCOT [61] для проведення самостійної оцінки рівня КБ;
– методика оцінки рівня КБ на підприємствах ядерного паливного циклу [62];
– методика оцінки стану КБ на основі оцінювання ключових показників [63] разом з методикою оцінки стану КБ методом анкетування [64].

В той же час програмні продукти для оцінки СЗІБ представлені, здебільшого, ризик-орієнтованими програмними комплексами. Так,

основними представниками серед програмних продуктів є OCTAVE [65], Risk Watch [66], ГРИФ [67], CORAS [68], CRAMM [69], Microsoft Security Assessment Tool [70], Oracle Crystal Ball [71]. Серед вище заданих продуктів підвищення поінформованості співробітників організації береться до уваги лише в OCTAVE (Таблиця 1.3).

Таблиця 1.3 – Порівняльні характеристики основних систем аналізу ризиків [65-71]

Критерій	CORAS	CRAMM	OCTAVE	Oracle Crystal Ball	RiskWatch	ГРИФ	MSAT
Загальні характеристики							
Орієнтація на організації різного розміру та галузь діяльності	+	+	+	+	+	+	+
Автоматизація «What-If»/ «Якщо»	н/в	-	-	+	+	н/в	-
Зручність сприйняття графіків та звітів	+	-	+	+	-	+	+
Простота використання	+	-	+	+	-	+	-
Безкоштовне використання	+	-	-	-	-	-	+
Підтримка	+	+	+	+	+	+	+
Кількісна оцінка	+	+	-	н/в	+	+	-
Якісна оцінка	+	+	+	н/в	-	+	+
Підвищення інформованості співробітників	-	-	+	н/в	-	н/в	н/в
Придатність до регулярного використання	-	+	+	н/в	н/в	н/в	+
Використання незалежної оцінки	+	+	-	н/в	н/в	+	+
Вхідні дані							
Ресурси	+	+	+	+	+	+	+
Тип інформаційної системи	н/в	+	+	-	+	-	н/в
Цінність ресурсів	+	+	+	н/в	+	+	н/в
Загрози	+	+	+	+	+	+	+
Вразливості системи	+	+	+	+	+	+	+
Вибір протидій	н/в	+	-	-	+	+	+
Базові вимоги в галузі ІБ	н/в	-	-	-	+	-	-
Втрати	н/в	-	-	-	+	-	-
Міри захисту	-	+	+	-	+	-	+
Частота виникнення загроз	н/в	-	-	-	+	-	-
Мережеве устаткування	н/в	-	+	-	-	+	н/в
Види інформації	н/в	-	н/в	-	-	+	н/в
Групи користувачів	н/в	-	-	-	-	+	+
Засоби захисту	н/в	-	+	-	-	+	+

Таким чином, стає очевидною відсутність надежної уваги до персональної КІБ співробітників організації, що є невід'ємною складовою організаційної культури, та автоматизованих систем її оцінки.

Ефективність впровадженої СІБ залежить від персоналу, особливо в таких питаннях, як необхідність дотримання вимог ІБ, відповідальність, розуміння потенційних наслідків інцидентів та сприйняття моніторингу ІБ [72], як показано на рисунку 1.10.

Рисунок 1.10 – Роль персоналу в СЗІБ організації [72]

Рівень КІБ організації можна оцінити, виходячи з основних показників ІБ, які супроводжують її бізнес-діяльність. Так, згідно ДСТУ ISO/IEC 27001:2015 (ідентичний до чинного ISO/IEC 27001:2013) [73] та ДСТУ ISO/IEC 27032:2016 (ідентичний до чинного ISO/IEC 27032:2012) [74], а також проаналізувавши систему показників культури безпеки для персоналу в галузі атомної енергетики, показниками КІБ можуть слугувати:

1) рівень ІБ-компетенції працівників:
   1.1) кваліфікація співробітників;
   1.2) наявність професійних ІБ-компетенцій та soft-компетенцій у мірі, що задовольняє вимоги згідно посади, що займає співробітник;

1.3) визначення напрямів подальшого розвитку фахівця для побудови індивідуальної траєкторії;

2) позиція адміністрації до проблеми КІБ та підтримка:

2.1) ІБ-політика організації;

2.1.1) наявність документально зафіксованих процесів та положень у вигляді ІБ-політики організації;

2.1.2) актуальність ІБ-політики;

2.1.3) обізнаність співробітників щодо ІБ-політики організації;

2.1.4) ІБ-політика організації доступна для стейкхолдерів через визначений порядок;

2.2) лідерство:

2.2.1) узгодженість ІБ-політики з метою та стратегією розвитку організації;

2.2.2) гарантії інтеграції СМІБ в процеси організації;

2.2.3) поінформованість щодо управління ІБ та відповідності вимогам СМІБ;

2.2.4) підтримка зусиль співробітників, спрямованих на розвиток СЗІБ;

2.2.5) стимулювання безперервного вдосконалення СЗІБ;

2.2.6) заохочення проявів лідерства на різних рівнях управління в межах встановленої відповідальності;

2.3) використання провідного досвіду;

2.4) інтеграція ІБ до внутрішніх процесів, що визначені організацією як важливі;

2.5) врахування ІБ-аспектів при договірній діяльності;

3) контроль над діями, що пов’язані з ІБ:

3.1) визначення меж та застосовність СМІБ для визначення областей впливу;

3.2) наявність СМІБ, підтримка та безперервне вдосконалення:

3.2.1) безперервне вдосконалення СЗІБ за результатами аудитів ІБ-ризиків;

3.2.2) оцінка результативності внесених змін до СЗІБ;

3.3) встановлення вимірюваних (за можливості) цілей щодо ІБ організації;

3.4) планування:

3.4.1) планування та проведення аудиту ІБ-ризиків;

3.4.2) безперервність дій, спрямованих на обробку ІБ-ризиків;

3.5) відповідність цілей актуальним вимогам до ІБ через оновлення;

3.6) аудит СЗІБ з врахуванням попередніх результатів.

4) комунікації:

4.1) зв’язки зі спеціалізованими спільнотами та галузевими кіберцентрами (ДССЗЗІ, кіберполіція, CERT-UA);

4.2) обмін досвідом (через навчання, семінари, вебінари, тренінги, круглі столи, тематичні лекції (що їх читають провідні спеціалісти в ІБ-галузі), школи, акції, спрямовані на підвищення обізнаності користувачів) тощо;

5) емоційний клімат:

5.1) конвергенція місії, стратегічного плану розвитку, цінностей організації з цінностями та індивідуальними траєкторіями співробітників;

5.2) розуміння цілей, потреб та вимог партнерів та підрядників.

Приведений вище перелік не претендує на повноту та може бути розширений додатковими показниками, що будуть вагомими з точки зору менеджменту, експертів та стейкхолдерів.

1.4 Невизначеність при описі об’єктів, що характеризують стан культури інформаційної безпеки організації

Проведення оцінки стану КІБ організації неминуче супроводжується таким неприємним явищем, як неповнота інформації.

За відсутності можливості здійснення інструментального оцінювання деяких параметрів КІБ найбільш зручним є використання якісних характеристик. В той же час деякі показники можуть залишатися недоступними для оцінки або ж не цікавити аудитора як індикатори стану. Таким чином, відображення поточного стану КІБ організації матиме деяку ступінь неточності. Не покращує ситуацію і проведення експертної оцінки, оскільки використання суб'єктивних думок також привносить певну невизначеність.

Для складних систем, до яких відноситься і КІБ організації, зберігають актуальність так звані НЕ-фактори [75]: невизначеність, неточність, нечіткість, – до яких можна додати випадковість. Н.Є. Муромець дає поняття невизначеності як "відсутність, неповнота, недостатність інформації про об'єкт, процес, явище, або непевність у вірогідності інформації" [75].

З врахуванням перелічених вище властивостей показників КІБ організації, їх оцінка вимагає спеціальних підходів, відмінних від методів класичної логіки. Ця проблема вирішується завдяки застосуванню методів нечіткої логіки (НЛ). Основною проблемою НЛ, що ускладнює використання таких методів в експертних системах і системах машинного навчання, є необхідність встановлення значень ймовірності або ступеня приналежності [76]. Згідно [77], неповнота інформації виражається у відсутності значень ряду характеристик опису системи. Підставами для неповноти інформації можуть бути [77]:

- неприйнятно великі трудомісткість або часові витрати на кількісну оцінку відповідних характеристик;
- принципова неможливість кількісної оцінки характеристик на даному рівні розвитку знань;
- погана організація служби інформації.

Як складова інформаційної системи оцінювання рівня КІБ організації розглядається блок оцінки стану особистої КІБ користувачів, якими є працівники. Оскільки особисті навички та знання в галузі ІБ безпосередньо

впливають на КІБ, виявлення «слабких місць» безпосередніх учасників інформаційного простору організації допоможе в подальшому визначити набір необхідних заходів щодо усунення вразливостей СЗІБ та розповсюдження основ КІБ серед працівників, що підсилить загальну КІБ організації. Отже, метою дослідження є визначення залежності загального рівня КІБ організації через КІБ співробітників на основі НЛ алгоритму з подальшим визначенням заходів та рекомендацій щодо підвищення рівня КІБ.

1.5 Постановка задачі та логічна структура роботи

Система управління культурою інформаційної безпеки (СУКІБ) є частиною загальної системи.

З метою побудови інформаційної системи для проведення оцінки рівня КІБ організації маємо вирішити наступні задачі:

1) Сформувати перелік первинних показників рівня культури інформаційної безпеки організації та її індикаторів.
2) Розробити модель інформаційних процесів обчислення рівня культури інформаційної безпеки організації.
3) Розробити елементи інформаційної технології визначення рівня культури інформаційної безпеки організації.
4) Провести експериментальне дослідження щодо збору та обробки первинної інформації для інформаційної технології оцінювання рівня культури інформаційної безпеки організації.

Загальна логічно-структурна модель роботи представлена на рисунку 1.11.

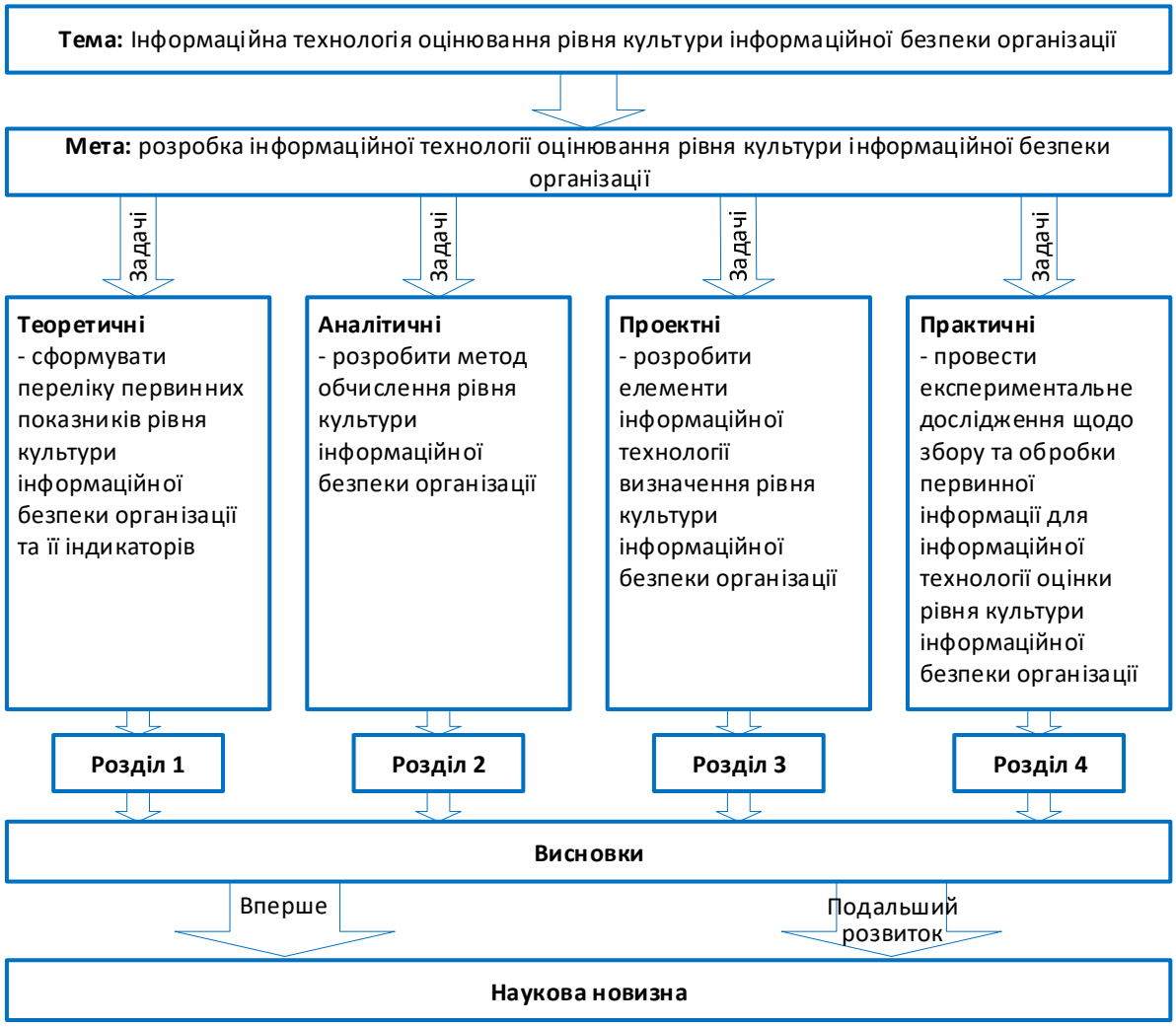

Рисунок 1.11 – Логічно-структурна модель дослідження

Для здійснення першого етапу дослідження пропонуємо виокремити наступні підзадачі:

1.1) Проведення аналізу інформаційної безпеки організації:
- дослідження методів оцінки ІБ;
- визначення системи ключових показників ІБ, що нададуть можливість отримати характеристику рівня КІБ організації технічним та кадровим забезпеченням;
- розробка моделі оцінки ІБ організації на базі вибраних показників.

1.2) Визначити структуру, формат вхідних та вихідних даних інформаційної системи.

1.3) Розробити спосіб розв’язання задачі – механізми та алгоритми ієрархічного нечіткого виводу.

Під час здійснення другого етапу на меті ставиться пропозиція структурно-функціонального рішення програмного комплексу аналізу КІБ організації.

Висновки до розділу 1

Аналіз сучасного стану ІБ на рівні організацій слугує підставою для наступних висновків:

1) Результати аналізу звітів за кіберінцидентами показали постійну присутність атак типу «man in the middle». Людина залишається в центрі уваги атакерів. Незважаючи на низку інцидентів зламу, складніші APT[2]-атаки пильно стежать за вразливістю людей. Відкритість та велика кількість інформації надає необмежені можливості для пошуку індивідуального підходу до жертви. Більшість користувачів соціальних мереж забувають про втрату контролю над особистою інформацією після її публікації в мережі. Крім того, користувачі забувають про ймовірність бути використаними для отримання, здавалося б, некритичної інформації, яка потім може бути використана для здійснення атаки, пов’язаної з їх професійною діяльністю.
2) Питання щодо впровадження та підтримки СМІБ виникає в наступних випадках:
   – бізнес-діяльність організації ефективно та успішно здійснюється завдяки використанню унікальних напрацьованих масивів інформації (бази даних, власні розробки, клієнтські персональні дані тощо) та за допомогою ІР на основі конфіденційних даних (онлайн-банкінг, медична база пацієнтів, адміністративна інформація тощо);

[2] Advanced Persistent Threat

– реалізація однієї із загроз (віддалена атака, помилка співробітника, збій системи підтримки ІР, саботаж та ін.) призвела до компрометації ІР з подальшими наслідками (фінансовими, іміджевими, адміністративними, кримінальними тощо).

3) Існуючі методи оцінки ІБ організацій пов’язані з певними ускладненнями із самими методологіями оцінки та невизначеністю характеристик, з якими доведеться зіткнутися експертам. Також, у випадку діяльності організації-початківця, чиї можливості обмежені досвідом та кваліфікацією працівників, невеликим бюджетом та рядом інших факторів, що відтісняють на другий план проблеми ІБ, розробка та впровадження СЗІБ покладена на ІТ-фахівців, здебільшого системних адміністраторів, що значно зменшує її ефективність.
4) Проблема формування КІБ організації на необхідному рівні може бути вирішена за допомогою використання підходів формування та підсилення корпоративної культури організації. Підсилення КІБ має бути засновано на підвищенні технологічної культури персоналу через підвищення обізнаності в галузі ІБ та залученні керівництва до розвитку КІБ організації.
5) З метою надання допомоги співробітникам ІТ-підрозділу, в якості набору основних рекомендацій щодо створення КІБ належного рівня, доцільною буде розробка інформаційної системи, яка дозволить визначити рівень наявної КІБ та сформувати ряд рекомендацій щодо усунення або зменшення ризиків, підсилення наявної СЗІБ організації.

Результати досліджень, приведених в розділі, опубліковані в роботах [18, 19, 20, 21, 23, 54, 55, 56, 72].

РОЗДІЛ 2
МАТЕМАТИЧНА МОДЕЛЬ ОЦІНКИ РІВНЯ КУЛЬТУРИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

2.1 Модель визначення вимог до рівня культури інформаційної безпеки персоналу на основі ІБ-ризиків

Для створення ефективної системи безпеки для приватного бізнесу та державних організацій і установ, необхідно вивчити та врахувати особливості персональної культури працівників, які мають різний рівень прав доступу до інформації. Необхідно також стежити за динамікою її змін та їх здатністю розрізняти та реагувати на атаки з використанням дезінформації. Це вимагає створення зручних та доступних інформаційних систем, які забезпечували б усі етапи управління КІБ, такі як:

1) дослідження існуючого рівня культури інформаційної безпеки організації;
2) визначення динаміки її зміни;
3) розробка заходів щодо підвищення рівня КІБ.

Водночас, питання автоматизації захисту інформаційних систем з врахуванням людських аспектів залишається недостатньо дослідженим. Вони в основному зосереджені на засобах виявлення технічної вразливості інформаційних систем людино-машинної взаємодії.

Така інформаційна система дозволить створити умови, необхідні для прийняття рішень щодо запобігання інформаційним впливам та своєчасного реагування.

Якщо для забезпечення захисту від зовнішніх порушників давно вже вироблені усталені підходи (хоча розвиток відбувається і в даному напрямку; про його інтенсивність свідчить різноманітність IDS[3]-систем, класифікація та принципи дії розглянуті в [78]), то методи протидії внутрішнім порушникам в

[3] Intrusion Detection System – система виявлення вторгнень

даний час все ще мають багато нерозглянутих питань. За результатом аналізу КІБ співробітника можна інтерпретувати як двокомпонентну систему: технічну та персональну складові.

Роль персоналу в процесі формування КІБ організації та підтримки наявної СЗІБ на практиці недооцінюють, адже від персоналу залежить ефективність впровадженої СЗІБ. Також впливовість персоналу проявляється у таких аспектах як необхідність дотримання вимог ІБ, відповідальність за стан КІБ, розуміння можливих наслідків інцидентів та сприйняття моніторингу ІБ.

Для визначення технічної складової вже розроблена велика кількість методик, які викладені в нормативній документації зі здійснення аудиту систем.

Типова методика включає виконання наступних основних етапів [79]:

- вивчення вихідних даних по АС;
- оцінка ризиків, пов'язаних із реалізацією загроз безпеки;
- аналіз механізмів безпеки організаційного рівня;
- аналіз конфігураційних файлів маршрутизаторів, мережевих екранів і проксі-серверів вручну;
- сканування зовнішніх мережевих адрес ЛОМ з мережі Інтернет;
- сканування ресурсів ЛОМ зсередини;
- аналіз конфігурації серверів і робочих станцій ЛОМ за допомогою спеціалізованих програмних засобів.

В таких підходах недостатньо виражене місце персональної КІБ адміністраторів та користувачів корпоративних мереж – представників другої складової.

Для врахування другої складової необхідно виконати такі основні дії:

- визначити вимоги до рівня персональної КІБ різних учасників інформаційних процесів в корпоративних мережах;
- оцінити рівень персональної КІБ, яка у більшості випадків є першопричиною виникнення загрози;

– розробити заходи з підвищення рівня КІБ учасників інформаційних процесів корпоративних мереж.

Загальна модель оцінки вимог до КІБ з врахуванням показників персональної безпеки та ризиків [72] наведена на рисунку 2.1.

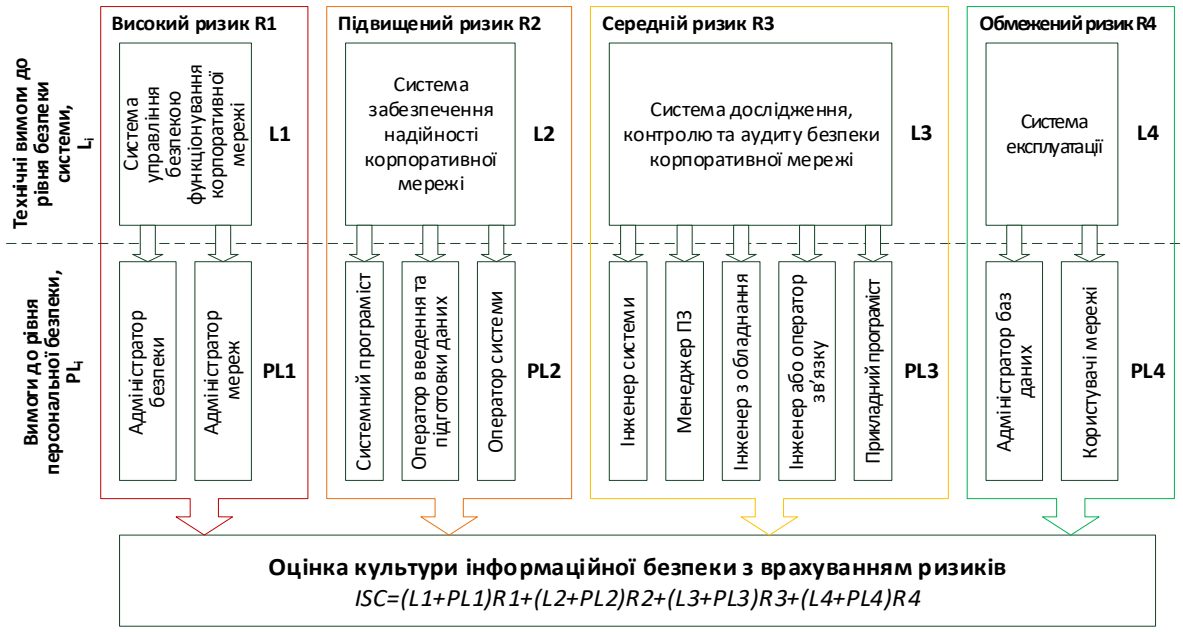

Рисунок 2.1 – Оцінка культури інформаційної безпеки з врахуванням показників персональної безпеки та ІБ-ризиків

Можливість застосування нечіткої моделі оцінки ризиків розглянуто та обґрунтовано в дослідженнях Alam & Pandey [80], Sallam [81], M. Al-Ali & A. AlMogren [82]. Наприклад, нечітка модель, що запропонована в [80], приймає до уваги рівень обізнаності користувачів щодо кіберзагроз, проте не зважає на їх посадові обов'язки в рамках виконуваних ролей. Модель зменшення ризиків, наведена в дослідженні [82], демонструє ефективність зменшення ризиків від ІБ-загроз з врахуванням сприйняття поточних ризиків учасниками інформаційних процесів (сприйняття, нейтральне ставлення або супротив).

Можливість проведення оцінки ІБ-ризиків за допомогою багаторівневої нечіткої моделі висвітлена в роботі [81]. Багатофакторна модель використовує лінгвістичні оцінки таких змінних як наміри, спрямованість, можливість, вразливість, ймовірність дій, ймовірність успішної реалізації загрози та

величина впливу. Проте не зважаючи на, здавалося б, вичерпний перелік факторів ризику, жодний показник явним чином не пов’язаний із персоналом.

Модель, що представлена на рисунку 2.1, приймає до уваги специфіку ролей користувачів, різні рівні ризику, а також визначення специфічних вимог до рівня КІБ персоналу.

Кожен зі вказаних вище користувачів відповідно до своєї категорії ризику може завдати більший або менший збиток системі. Відзначимо, що причини виникнення нестандартних ситуацій можуть мати випадковий або навмисний характер, причому, попри інсайдерську діяльність або помсту, найчастіше причинами стають легковажність, необачність, цікавість, лінь, жадібність та нетерплячість – риси, природньо притаманні людині.

Отже, чим вищий рівень управління КС, тим сильніший його вплив і більша персональна відповідальність, що мають враховуватися при визначенні загального показника інформаційної безпеки комп’ютерної мережі (ІБКМ).

Визначення персональної КІБ на першому етапі пропонується проводити методами нечіткої логіки, оскільки проведення вимірювань показників неможливе інструментальним шляхом та має складність подальшої формалізації. Вказані проблеми нівелюються при використанні емпіричних (експертних) методів, але ті, в свою чергу, привносять неточність при визначенні вхідних показників.

2.2 Модель оцінки рівня персональної культури інформаційної безпеки

Важливість посилення людського фактору за рахунок підвищення рівня КІБ зумовлена можливістю настання катастрофічних наслідків в результаті виникнення ІБ-інцидентів, особливо на об'єктах критичної інфраструктури.

Під час аудиту СМІБ організації слабко формалізовані методи оцінки КІБ працівників у загальній системі ІБ організації. Слід зазначити, що апаратні системи захисту спрямовані на реагування та усунення наслідків ІБ-інцидентів

лише відомих атак, а виявлення та реагування на атаки нових типів є функцією персоналу.

Таким чином, неподільність персональної КІБ працівників (як користувачів та учасників внутрішнього інформаційного простору організації) та організаційної КІБ є основою для подальшого вивчення персональної КІБ.

Велика кількість індикаторів персональної КІБ, наведених в п.1.3, може забезпечити оцінювання наявних у користувача ІБ-компетенцій, проте, з огляду на мінливу ситуацію, яка щодня викриває нові загрози, модель оцінки персональної КІБ повинна бути адаптивною. Подібна задача легко вирішується за допомогою ієрархічної нечіткої моделі. Це дозволить легко створювати та коригувати базу правил (БП) на випадок зміни характеристик реальної системи, доповнення лінгвістичної моделі або нових варіантів рішення. При розробці бази знань в основу покладено набір продукційних правил на основі системи нечітких висновків (FIS/CHB).

Оскільки модель персональної КІБ користувача (співробітника, цифрового партнера, посередника) не може бути формалізована точними математичними методами, для вирішення цієї проблеми можуть використовуватися інтелектуальні методи, що базуються на системі людських висновків.

В якості математичного апарату для визначення рівня обізнаності ми використовуємо положення нечіткої логіки [83] та теорію нечітких множин. Такий підхід дозволяє уникнути необхідності кількісної оцінки показників, замінюючи їх якісними характеристиками у вигляді фразових висловлювань. За допомогою цього методу були ефективно розв’язані задачі формалізації в роботах Адітія П. Сінгха та Праділа Томара (Aditya P. Singh and Pradeep Tomar) [84], Ашиша Кумара Харе, Дж. Л. Рани та Р. К. Джейна (Ashish Kumar Khare, J. L. Rana and R. C. Jain) [85], Хані Ф. Атлама та ін. (Hany F. Atlam et. al.) [86].

Таким чином, використання нечіткої логіки вирішує проблеми, пов'язані з неточністю визначення кількісних характеристик, невизначеністю опису ситуації тощо.

Оскільки вкрай важко отримати точні або принаймні числові вхідні змінні в такій галузі, як КІБ, а також встановити формальні залежності між входами та результуючою змінною, вирішено скористатися нечіткими логічними методами, побудованими на алгоритмі Мамдані [87]. База правил прозора і зрозуміла; робить правила доступними для редагування. Це дозволяє легко інтерпретувати терми, які зрозумілі не тільки для розробників, але і для користувачів.

Для формування нечіткої системи для оцінки базового рівня персональної КІБ користувача використано обчислювальне середовище MATLAB Fuzzy Logic Designer [88]. При формуванні нечіткої моделі було вирішено вдатися до ієрархічного принципу побудови, оскільки він дає змогу зменшити кількість правил і легко оперувати залежностями проміжних змінних на кількох входах [89]. Модель визначення рівня персональної КІБ представлена трьома підсистемами [90, 91], які відповідають тематичним трійкам вхідних змінних, та результуючою підсистемою на основі трьох проміжних вихідних змінних згаданих підсистем нижчого ієрархічного рівня (рисунок 2.2).

На рисунку 2.2 представлена ієрархічна система, яка моделює залежність $y_4 = f(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9)$ за допомогою чотирьох баз знань. Представлені бази знань описують залежності $y_1 = f(x_1, x_2, x_3)$, $y_2 = f(x_4, x_5, x_6)$, $y_3 = f(x_7, x_8, x_9)$ та результуюча підсистема $y_4 = f(y_1, y_2, y_3)$.

Для опису змінних вибрано трикутні функції належності (ФН). Застосування трикутних ФН обґрунтовано тим, що запропоновані варіанти відповіді на питання (лінгвістичну змінну) інтерпретуються як терми без процедури фазифікації. При отриманні відповіді на певне питання, вона сприймається як відповідний терм зі значенням ФН $\mu_{T_j}(x_i) = 1$. Змінні x_1, x_2,

x_4, x_5, x_7, x_8 характеризуються трьома термами (Рисунок 2.3). Змінні x_3, x_6, x_9, y_1, y_2, y_3, y_4 запропоновано описати п'ятьма термами (Рисунок 2.4).

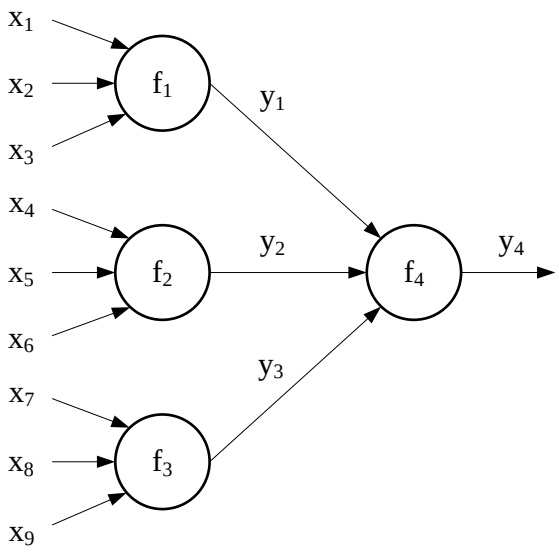

Рисунок 2.2 – Ієрархічна нечітка база знань

Лінгвістичні змінні, терми, їх інтерпретація та ФН приведені в Додатку Б.

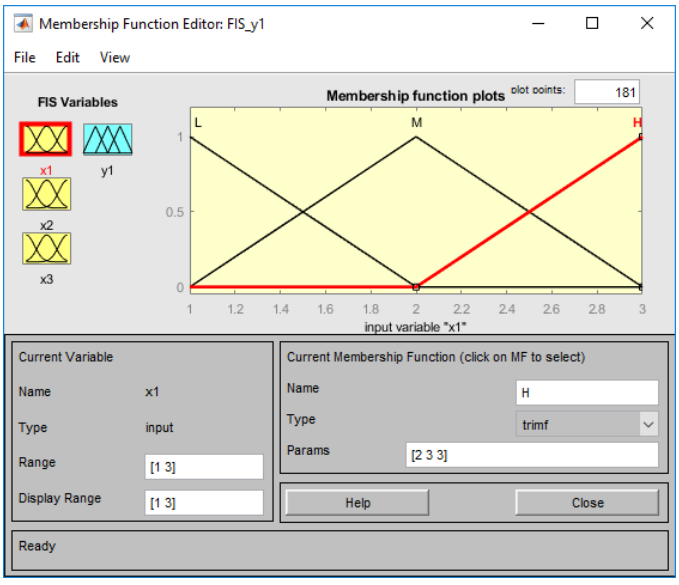

Рисунок 2.3 – Функції належності для змінної $x1$ системи Fis_y1

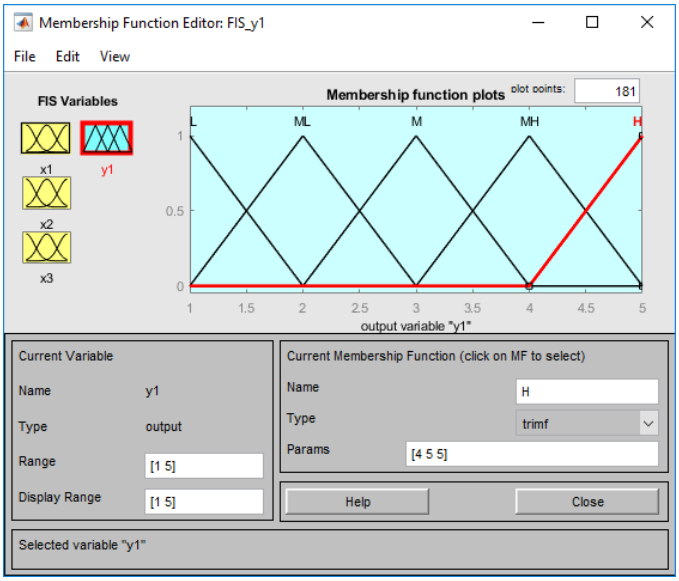

Рисунок 2.4 – Функції належності для змінної $x3$ системи $Fis\_y1.fis$

При цьому, наприклад, для змінної $x1$:

– терм L відповідає варіанту відповіді на питання у вигляді – «Я користуюся одним аккаунтом, ноутбуком і смартфоном, ціную мобільність і переваги синхронізації»;

– терм M відповідає відповіді на питання у вигляді – «Грань між робочими й особистими гаджетами дуже умовна, але я намагаюся їх розділяти»;

– терм H відповідає варіанту – «Використовую робочий ноутбук, телефон і окрему поштову адресу».

Фрагмент створеної БП для першої підсистеми нечіткого логічного виводу $y1 = f(x1, x2, x3)$ в редакторі БЗ наведений на рисунку 2.5; візуалізація нечіткого логічного виводу наведена на рисунку 2.6.

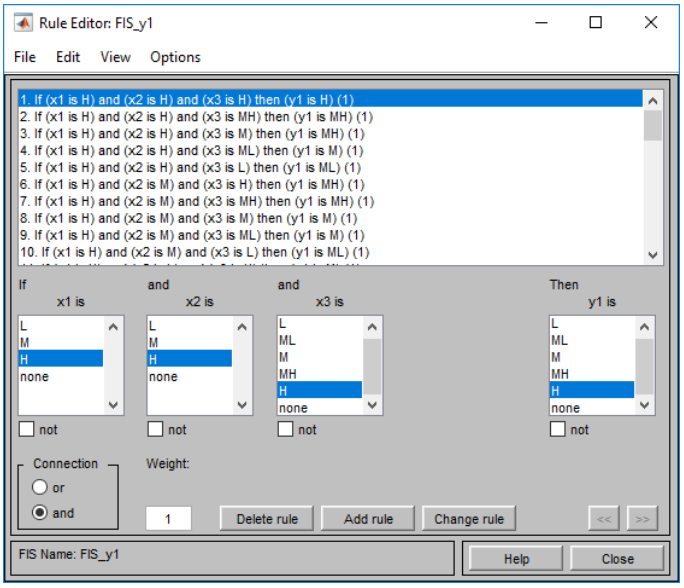

Рисунок 2.5 – База правил нечіткої підсистеми $Fis\_y1.fis$ в редакторі бази знань

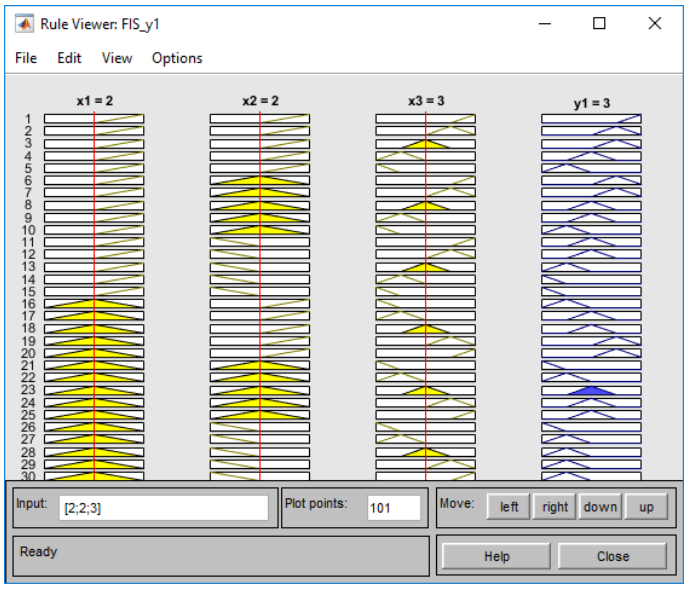

Рисунок 2.6 – Візуалізація нечіткого логічного виводу підсистеми $Fis\_y1.fis$

Контроль коректності та повноти створеної БП першої підсистеми можливий завдяки моделюванню поверхні «входи – вихід» (рисунок 2.7, рисунок 2.8).

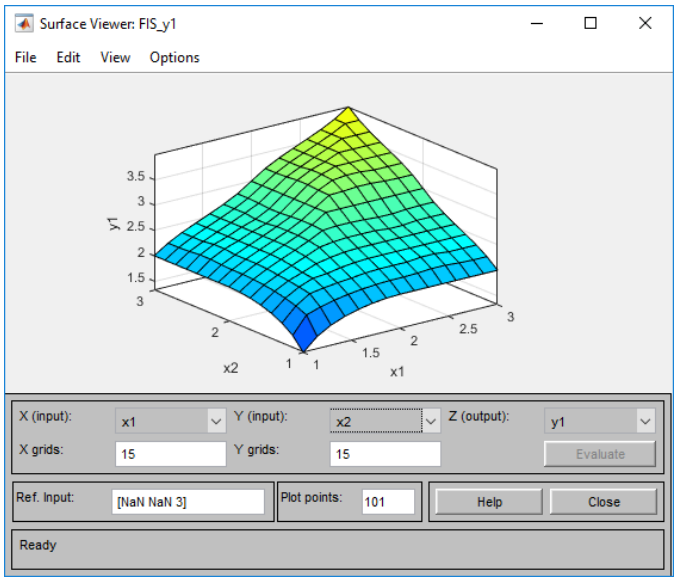

Рисунок 2.7 – Поверхня «входи – вихід» $y1 = f(x1, x2)$

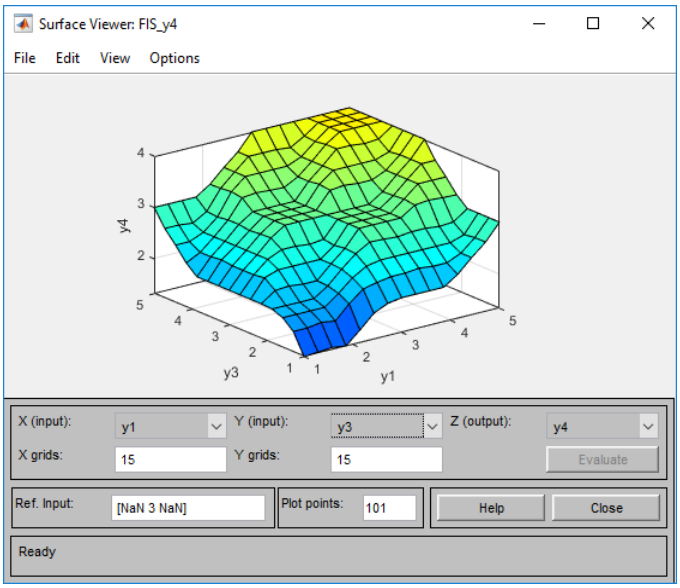

Рисунок 2.8 – Поверхня «входи – вихід» для результуючої нечіткої підсистеми $Fis\_y4.fis$

В результаті формування БП ієрархічної нечіткої системи було створено 45 правил для підсистеми $Fis\_y1.fis$, 31 правило для підсистеми $Fis\_y2.fis$, 45 правил для підсистеми $Fis\_y3.fis$ та 105 – для підсистеми вищого рівня $Fis\_y4.fis$.

Переваги обраного підходу до оцінювання рівня персональної КІБ користувачів можна побачити в ясності та простоті впровадження, зручності коригування бази даних у разі необхідності внесення змін, можливості

використання штучного інтелекту при оцінці КІБ, яка не піддається машинній логіці. Серед недоліків можна відмітити експертну суб’єктивність при складанні БП. Цей недолік можна зменшити залученням до участі групи експертів з використанням коефіцієнту конкордації для перевірки збігу їх суджень.

2.3 Модель оцінки рівня культури інформаційної безпеки організації

В рамках діяльності організації кожен з працівників виконує певні робочі функції, в тому числі в галузі ІБ. Залежно від цього формуються певні вимоги до компетенцій, що забезпечують визначений рівень КІБ у процесі виконання функціональних обов'язків.

Джерелом для формування питань може виступати міжнародний стандарт ISO/IEC 27001. Враховуючи діяльність організації та її працівників, також може бути задіяний стандарт ISO/IEC 27032.

Ієрархічна шестирівнева нечітка модель оцінки рівня КІБ персоналу організації [92] може бути представлена у вигляді двох підсистем, кожна з яких має окремі функції, а саме: підсистема 1 – ранжування факторів (1-й та 2-й рівні) та підсистема 2 – визначення інтегрального показника рівня КІБ організації (3–6-й рівні), як показано на рисунку 2.9.

Слід зазначити, що система є циклічною, оскільки процес підвищення рівня КІБ є безперервним, а оцінка рівня КІБ повинна відбуватися в рамках ІБ-аудиту організації. Необхідність регулярного ІБ-аудиту полягає в постійній оцінці реального стану ІБ та/або інформаційних ресурсів та їх здатності протистояти зовнішнім та внутрішнім ІБ-загрозам, які постійно змінюються та адаптуються.

У той же час ІБ-аудит є систематичним процесом отримання об'єктивних кількісних та якісних оцінок поточного стану безпеки інформаційної системи. Він здійснюється з урахуванням трьох основних факторів: персоналу, процесів та технологій.

Для цього потрібно сформувати єдиний інтегральний показник КІБ організації D_{org}. Для вирішення проблеми пропонується використовувати нечіткі методи прийняття рішень, які дозволяють моделювати плавні зміни властивостей об'єкта, а також відобразити функціональні залежності, що не піддаються формалізації математичними методами.

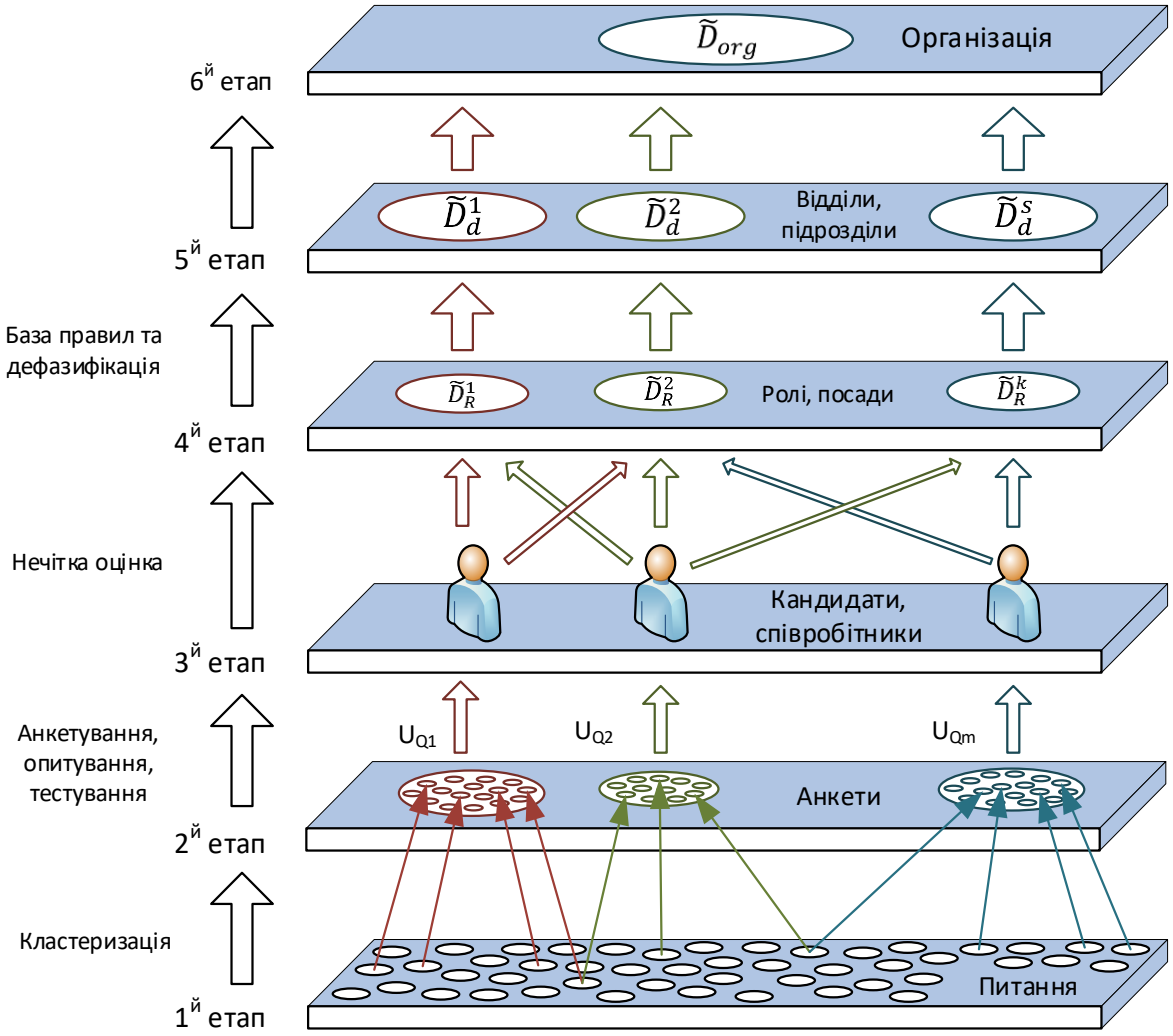

Рисунок 2.9 – Модель оцінки рівня КІБ організації

Отже, у математичному вигляді модель оцінки рівня КІБ організації представляє собою мультиплікаційну згортку (2.1):

$$f: C_1 \times C_2 \times \ldots \times C_m \times \tilde{Q}_1(T) \times \tilde{Q}_2(T) \times \ldots \times \tilde{Q}_n(T) \to \widetilde{D}_{org} = \{\widetilde{D}_d^1, \widetilde{D}_d^2, \ldots, \widetilde{D}_d^s\}, \quad (2.1)$$

де $C_1, C_2, \ldots, C_m$ – масив ІБ-компетенцій персоналу;

$\tilde{Q}_1(T), \tilde{Q}_2(T), \ldots, \tilde{Q}_n(T)$ – масив нечітких відповідей на питання;

$\widetilde{D}_d^1, \widetilde{D}_d^2, \dots, \widetilde{D}_d^s$ – масив нечітких інтегральних показників КІБ структурних підрозділів організації;

$\widetilde{D}_{org}$ – нечіткий показник КІБ організації.

Зауважимо, що при побудові моделі формування лінгвістичної оцінки рівня КІБ вхідними змінними виступають кількісні фактори (m – кількість компетенцій; n – кількість питань; r – кількість службовців; s – кількість підрозділів); і якісні ($Q_i(T)$ – лінгвістичні оцінки відповідей на питання ($j = 1, \dots, n$) з набором термів, наприклад, {поганий, нормальний, хороший} або {низький, середній, високий}).

Системи нечітких продукцій реалізуються згідно методу нечіткого логічного виводу, запропонованого Р. Беллманом та Л. Заде [93]. Оцінку рівня КІБ можна забезпечити за допомогою пакету MATLAB Fuzzy Logic Designer.

Перший етап наведеної моделі – формування множини питань (Рисунок 2.10).

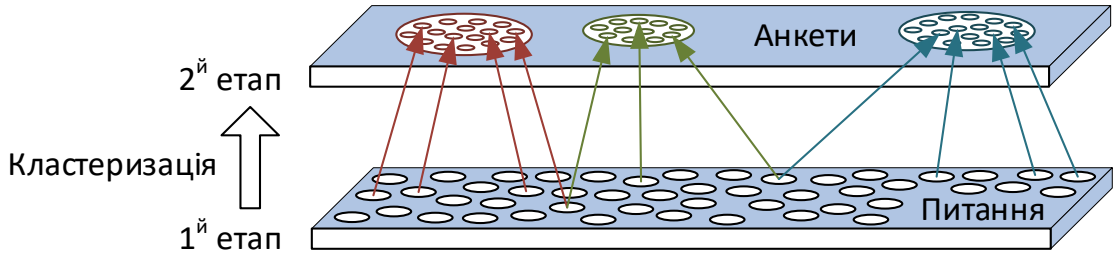

Рисунок 2.10 – Кластеризація питань при формуванні анкет

На першому етапі формують масив факторів (компетенцій) $U_C = \{C_1, C_2, \dots, C_m\}$, який містить ІБ-компетенції, та масив індикаторів (набір питань) $U_Q = \{Q_1, Q_2, \dots, Q_n\}$, що характеризують об’єкт дослідження (КІБ). Відмітимо, що компетенція включає знання та розуміння того, як діяти та як бути; визначена предметною областю, в якій індивід добре поінформований, та в якій він готовий здійснювати безпечну діяльність.

Оцінювання компетенцій може здійснюватися за допомогою анкетування (тестування), що відображає ІБ-діяльність працівника. Ці компетенції можуть бути визначені вимогами до кваліфікації фахівців

відповідно до їх спеціальності, а також можуть бути сформовані на окремих робочих місцях залежно від ролей, що виконуються в рамках загальної системи безпеки.

Формування масиву компетенцій та питань може залежати від різних груп користувачів. Це можуть бути інженери інформаційної безпеки організації, керівники відділів безпеки або керівники організації.

Другий етап. Створення набору критеріїв (кластерів) $C^i: Q^i \subset U_Q$, що характеризують окремі компетенції для відповідних наборів питань. При цьому в межах кожної окремої компетенції набір питань має якісно однорідні показники, які формуються на основі виду професійної діяльності співробітника.

Враховуючи умови для формування кластерів, найбільш доцільним методом кластеризації є нечітка кластеризація. Цей метод дозволяє включати один і той же об'єкт (питання, що виступає в ролі змінної) до подібних компетенцій. В результаті кластеризації готуються анкети або тести для опитування працівників.

В межах кожного набору компетенцій $C^i: Q^i \subset U_Q$ завдання полягає у визначенні відповідних ваг питань, які його формують. Мета цього завдання – визначити вагу їх впливу на елементи наступних рівнів ієрархії.

Це доцільно реалізувати завдяки використанню методу парних порівнянь [94], тобто шляхом попарного порівняння ваг питань за відповідною шкалою. Таким чином, для кожної компетенції C^i з набору $\{C_1, C_2, \dots, C_m\}$ буде сформована матриця парних порівнянь множини питань $Q^i = \left(q_{ij}^i\right)$, на основі якої визначається їх відносний ваговий вектор $\left\{w_1^i, w_2^i, \dots, w_n^i\right\}$, та матриця парних порівнянь $C = c_{ij}$ сукупності компетенцій, на основі якої визначає вагу кожної компетенції $W = \{W_1, W_2, \dots, W_m\}$.

Вага кожної ролі P (ієрархія ролей відома заздалегідь) визначається за допомогою принципу Фішберна [95] за формулою:

$$P_k = \frac{2\cdot(r-k+1)}{(r+1)\cdot r}, \qquad (2.2)$$

де P_k – ваговий коефіцієнт i-ої ролі (посади);

r – кількість посад (ролей);

k – порядковий номер (ранг/індекс) посади.

Третій етап. За результатами 1-го та 2-го етапів визначається персональний рівень КІБ спеціалістів (рисунок 2.11).

Зауважимо, що при визначенні персонального рівня КІБ вагу W_i кожної i-ї компетенції вважаємо рівними, тобто вони дорівнюють $1/m$, іншими словами, загальна нечітка оцінка персонального рівня КІБ фахівця визначається за формулою:

$$\widetilde{D}_p = \sum_{i=1}^{m}\sum_{j=1}^{n_j}\frac{1}{m}\cdot w_{ij}\cdot \tilde{Q}(T)_{ij}, \qquad (2.3)$$

де m – кількість компетенцій;

n_i – кількість питань для i-ої компетенції;

w_{ij} – вага j-го питання, що відноситься до i-ої компетенції;

$\tilde{Q}(T)_{ij}$ – лінгвістична оцінка j-го питання за i-ою компетенцією.

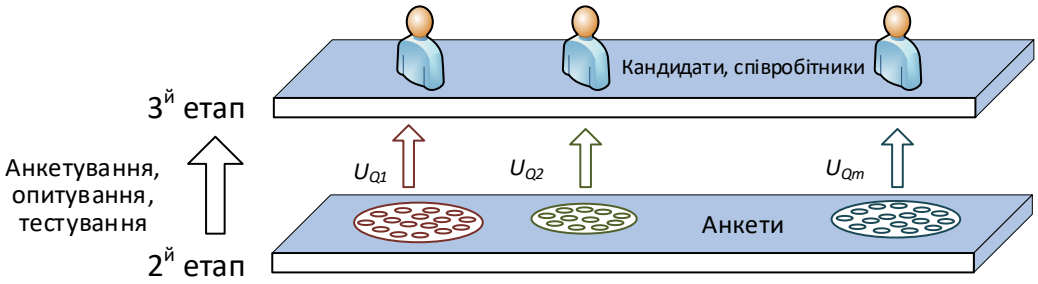

Рисунок 2.11 – Формування набору анкет

Четвертий етап. Оскільки різні ролі виконуються на різних рівнях ІБ організації, (наприклад, користувач, підтримка систем безпеки, управління безпекою тощо), вимоги до їх ІБ-компетенцій будуть різними.

Отже, в рамках діяльності організації (відділу) кожен працівник виконує певні функції (ролі) в системі захисту інформації, які визначаються відповідним набором компетенцій $C = \{c^1, c^2, \ldots, c^m\}$. Навчання, досвід та кваліфікація всіх осіб, які беруть участь у будь-яких заходах, пов'язаних з

повним життєвим циклом ІБ, повинні оцінюватися для конкретного випадку. Для оцінки компетентності осіб під час виконання своїх обов'язків (ролей) для кожної посади слід сформувати власний набір компетенцій $R^k: C^j \subset U_C$.

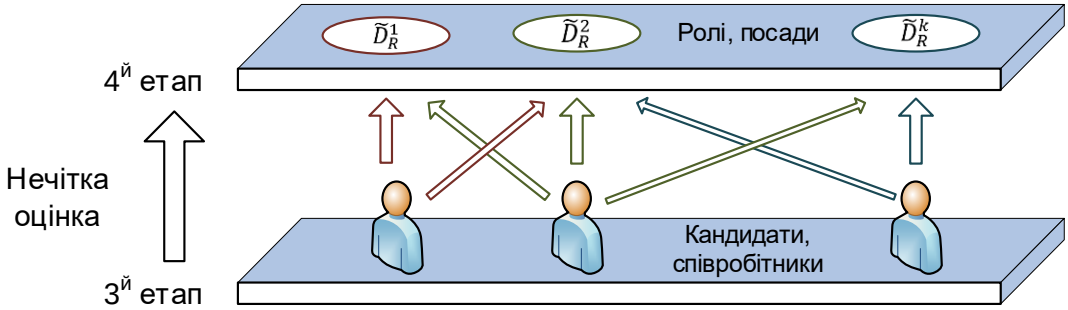

Рисунок 2.12 – Оцінка рівня КІБ в рамках посади на основі персональної КІБ співробітника

Загальна нечітка оцінка КІБ для ролі/посади $\widetilde{D}_R$ (ступінь) визначається за формулою:

$$\widetilde{D}_R = \sum_{i=1}^{m} \sum_{j=1}^{n_i} W_i \cdot w_{ij} \cdot \tilde{Q}\,(T)_{ijk}, \qquad (2.4)$$

де m – кількість компетенцій;

n_i – кількість питань в галузі i-ої компетенції;

W_i – вага i-ої компетенції;

w_{ij} – вага j-го питання стосовно i-ої компетенції;

$\tilde{Q}(T)_{ijk}$ – лінгвістична оцінка j-го питання i-ої компетенції для k-ої ролі (посади).

П'ятий етап. Загальна нечітка оцінка КІБ відділу $\widetilde{D}_d$ визначається за формулою:

$$\widetilde{D}_d = \sum_{i=1}^{r} P_k \cdot \widetilde{D}_R^k, \qquad (2.5)$$

де r – кількість посад (ролей);

P_k – вага i-ої ролі (посади);

$\widetilde{D}_R^k$ – оцінка (кількісна, якісна) k-ої ролі.

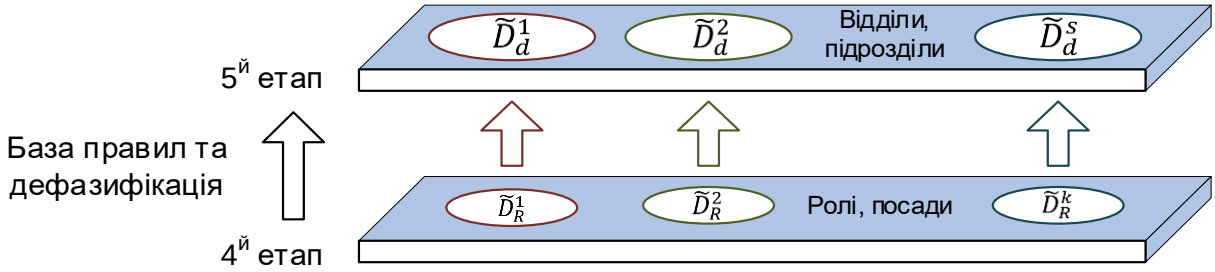

Рисунок 2.13 – Визначення рівня КІБ структурного підрозділу на основі показників рівня КІБ за відповідними посадами

Шостий етап. Інтегральний показник рівня КІБ організації $\widetilde{D}_{org} = \{\widetilde{D}_d^1, \widetilde{D}_d^2, \dots, \widetilde{D}_d^s\}$ визначається як середнє геометричне значення інтегральних показників відділів:

$$\widetilde{D}_{org} = \sqrt[s]{\widetilde{D}_d^1 \cdot \widetilde{D}_d^2 \cdot \dots \cdot \widetilde{D}_d^s}. \quad (2.6)$$

Показники $\widetilde{D}_R$, $\widetilde{D}_d$, $\widetilde{D}_{org}$ можна розглядати як функції часу $\widetilde{D}_R(t)$, $\widetilde{D}_d(t)$, $\widetilde{D}_{org}(t)$, тобто в динаміці. Це дає можливість проаналізувати часовий ряд відповідних функцій, отриманих за певний проміжок часу. Вони характеризують зміну КІБ для посади, відділу, організації залежно від реальних результатів навчання та засвоєних уроків, а їх тенденції визначають напрямок змін. Аналіз тенденцій може виявитись дуже корисним як для організації в цілому, так і для працівників, зокрема, дозволяє зробити висновок про сучасний та майбутній стан КІБ та ефективність запропонованих навчальних курсів та інших заходів інформаційної безпеки.

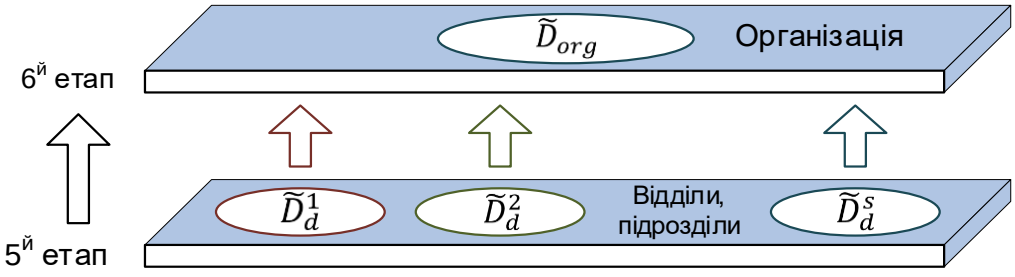

Рисунок 2.14 – Визначення інтегрального показника рівня КІБ організації

Загальна формула для визначення ефективності запропонованих навчальних курсів та інших заходів щодо вдосконалення ІБ:

$$E_{ff} = \frac{\widetilde{D}(t_{curr})}{\widetilde{D}(t_{prev})}. \quad (2.7)$$

Результати розрахунків у динаміці будуть відображати ефективність управління безпекою особового складу.

2.4 Методи та алгоритми інформаційної технології оцінювання рівня КІБ організації

2.4.1 Нечітка кластеризація

Для проведення оцінки КІБ персоналу, як елемента загальної моделі оцінки КІБ організації, необхідно сформувати набір анкет, які будуть визначати рівень наявних ІБ-компетенцій персоналу відповідно до їх ролей в інформаційних процесах організації.

Алгоритм нечіткої кластеризації дозволяє віднести один об’єкт до декількох кластерів, спираючись на матрицю нечіткого розбиття [89], що попередньо визначена експертом. Кластеризація може відбуватися за допомогою алгоритмів k-середніх та c-середніх. Оскільки дана задача полягає у створенні кластерів, що стосуються певних тем в галузі інформаційної безпеки, та можливості віднесення тих самих питань до різних тематик, пропонується застосовувати алгоритм нечіткої кластеризації c-means [96, 97].

Формування анкет для різних ролей здійснюється з врахуванням вимог до компетенцій працівників залежно від їх ролі у забезпеченні загальної системи безпеки організації. Суттєвою перевагою такого підходу є можливість реалізації оцінювання КІБ організації, виходячи зі специфіки її функціонування.

В даному випадку алгоритм кластеризації c-means буде здійснюватися наступним чином:

– кількість кластерів j обумовлена кількістю тематик T_j, за якими проводиться дослідження. Це можуть бути питання технічної, технологічної та персональної інформаційної безпеки ($j = \overline{1,t}$).

– експертна оцінка формує матрицю нечіткого розбиття F, що містить дані про ступінь належності μ_{Q_i} питання Q_i $(i = \overline{1,n})$ до тематики-кластеру T_j. Її можна описати у вигляді:

$$F = \left[\mu_{Q_i j}\right], \mu_{Q_i j} \in [0,1], i = \overline{1,n}, j = \overline{1,t}, \quad (2.8)$$

де i-тий рядок містить ступені належності питання Q_i до кластерів T_j. Обов'язковою умовою для матриці нечіткого розбиття є обмеження:

$$0 < \sum_{i=\overline{1,n}} \mu_{Q_1 j} < n, j = \overline{1,t}. \quad (2.9)$$

– центри кластеру задаються питаннями, які мають максимальне значення ступеню належності μ_{Q_i} до певної тематики T_j.

Далі реалізація нечіткої кластеризації проводиться за відомим алгоритмом [89].

Вихідними даними для формування анкет оцінки КІБ працівника є множина питань (джерело – стандарт ISO/IEC 27001, можливе також використання стандарту ISO/IEC 27032 згідно умов діяльності організації); перелік тем і тематик, що дозволять охопити напрями професійної діяльності певного працівника; набір ролей, що виконуються працівником при обійманні певної посади; та набору компетенцій, що мають бути опановані претендентом.

В якості основи для оцінки результатів тестування використовуються матриці ІБ-компетенцій.

2.4.2 Методи нечіткої логіки для оцінки результатів анкетування

Складність та багатофакторність системи, що може бути представлена завдяки моделі КІБ організації, зумовлює доцільність використання ієрархічного підходу, завдяки чому стає простіше та менш витратно за часом та зусиллями створити декілька БП початкового рівня з подальшим формуванням БП наступного рівня.

Спираючись на роботи С.Д. Штовби [98], ми маємо можливість скористатися основними перевагами ієрархічних нечітких БЗ. Першою

перевагою є здатність подолати «прокляття розмірності» через скорочення кількості нечітких правил для коректного опису моделі з багатьма вхідними змінними. Друга – наочність отриманої моделі та її інтерпретабельність.

2.4.2.1 Системи ієрархічного нечіткого логічного виводу

Природа самого явища КІБ організації не передбачає можливість здійснювати інструментальне вимірювання показників, що зумовлює використання лінгвістичних змінних та набору правил, що якнайбільш повноцінно описують модель. Нетренована людина здатна тримати у пам'яті 7±2 характеристики об'єкту (чанки) [99, 100], що буде прийнято до уваги під час формування нечітких підсистем.

Так, наприклад, для опису моделі з дев'ятьма вхідними змінними, представленої на рисунку 2.2, що описана залежністю $y_4 = \mathrm{f}(\mathrm{x}_1, \mathrm{x}_2, \mathrm{x}_3, \mathrm{x}_4, \mathrm{x}_5, \mathrm{x}_6, \mathrm{x}_7, \mathrm{x}_8, \mathrm{x}_9)$, використані три підсистеми початкового рівня $y_1 = \mathrm{f}(\mathrm{x}_1, \mathrm{x}_2, \mathrm{x}_3)$, $y_2 = f(\mathrm{x}_4, \mathrm{x}_5, \mathrm{x}_6)$, $y_3 = \mathrm{f}(\mathrm{x}_7, \mathrm{x}_8, \mathrm{x}_9)$ та результуюча підсистема $y_4 = \mathrm{f}(\mathrm{y}_1, \mathrm{y}_2, \mathrm{y}_3)$.

За умов, що кожна вхідна лінгвістична змінна описується трьома термами, максимальна кількість правил для нечіткої системи $y_4 = \mathrm{f}(\mathrm{x}_1, \mathrm{x}_2, \mathrm{x}_3, \mathrm{x}_4, \mathrm{x}_5, \mathrm{x}_6, \mathrm{x}_7, \mathrm{x}_8, \mathrm{x}_9)$ дорівнюватиме $3^9 = 19\,683$. За умов, що результуючі вихідні змінні характеризуються, наприклад, п'ятьма термами, то для ієрархічної нечіткої бази правил їх максимальна кількість скоротиться до $3^3 + 3^3 + 3^3 + 5^3 = 206$.

При побудові ієрархічної нечіткої системи існує два можливі варіанти передачі виходів від нижньої підсистеми на вхід верхньої [89]. Перший спосіб реалізує трансляцію результату логічного виводу після дефазифікації. За другим способом передається результат логічного виведення до дефазифікації, тобто нечітка множина [98]. У першому випадку недоліками є необхідність проведення проміжних операцій дефазифікації та фазифікації, потреба встановлення ФН, а також дотримання еквівалентності нечітких множин до та після операцій дефазифікації та фазифікації. Проте це компенсується

простотою побудови ієрархічного зв'язку та здатністю застосувати типові алгоритми як, наприклад, за допомогою пакету Fuzzy Logic Designer математичного середовища MATLAB. Другий спосіб побудови ієрархічного зв'язку виключає проміжні операції дефазифікації та фазифікації. За таких умов результат логічного виводу формується у вигляді нечіткої множини та спрямовується до машини нечіткого виводу наступного рівня ієрархії. Це також виключає необхідність присвоєння функцій належності для проміжних змінних, залишаючи при цьому вимогу до еквівалентності терм-множин.

2.4.2.2 Математична модель ієрархічного нечіткого виводу

Для опису математичної моделі нечіткого ієрархічного виводу для моделі, наведеної на рисунку 2.2, використаємо згадані раніше позначення $y_1 = \mathrm{f}(\mathrm{x}_1, \mathrm{x}_2, \mathrm{x}_3),\ y_2 = f(\mathrm{x}_4, \mathrm{x}_5, \mathrm{x}_6),\ y_3 = \mathrm{f}(\mathrm{x}_7, \mathrm{x}_8, \mathrm{x}_9)$ для підсистем нижчого рівня та результуючої підсистеми $y_4 = \mathrm{f}(\mathrm{y}_1, \mathrm{y}_2, \mathrm{y}_3)$.

$$\bigcup_{p=1}^{k_j}\left(\bigcap_{i=1}^{3} x_i = a_{i,jp} \text{ з вагою } w_{jp}\right) \rightarrow y_1 = d_j,\ j = \overline{1,m} \qquad (2.10)$$

$$\bigcup_{p=1}^{k_j}\left(\bigcap_{i=4}^{6} x_i = a_{i,jp} \text{ з вагою } w_{jp}\right) \rightarrow y_2 = d_j,\ j = \overline{1,m} \qquad (2.11)$$

$$\bigcup_{p=1}^{k_j}\left(\bigcap_{i=7}^{9} x_i = a_{i,jp} \text{ з вагою } w_{jp}\right) \rightarrow y_3 = d_j,\ j = \overline{1,m} \qquad (2.12)$$

$$\bigcup_{p=1}^{k_j}\left(\bigcap_{i=1}^{3} y_i = a_{i,jp} \text{ з вагою } w_{jp}\right) \rightarrow y_4 = d_j,\ j = \overline{1,m} \qquad (2.13)$$

За композиційним правилом Заде отримуємо вираз:

$$\tilde{y}_1 = \tilde{A}(x_1, x_2, x_3) \circ R(x_1, x_2, x_3, y_1), \qquad (2.14)$$

$$\tilde{y}_2 = \tilde{A}(x_4, x_5, x_6) \circ R(x_4, x_5, x_6, y_2), \qquad (2.15)$$

$$\tilde{y}_3 = \tilde{A}(x_7, x_8, x_9) \circ R(x_7, x_8, x_9, y_3), \qquad (2.16)$$

$$\tilde{y}_4 = \begin{pmatrix} \tilde{A}(x_1, x_2, x_3) \circ R^1(x_1, x_2, x_3, y_1), \\ \tilde{A}(x_4, x_5, x_6) \circ R^1(x_4, x_5, x_6, y_2), \\ \tilde{A}(x_7, x_8, x_9) \circ R^1(x_7, x_8, x_9, y_3) \end{pmatrix} \circ R^2(y_1, y_2, y_3, y_4) \qquad (2.17)$$

або

$$\tilde{y}_4 = \left(\tilde{A}(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9) \circ R^1(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, y_1, y_2, y_3)\right) \circ R^2(y_1, y_2, y_3, y_4). \qquad (2.18)$$

Оператор $fuzzy\ \tilde{x}_i = fuzzy(x_i) = \left[\mu_{x_i}, x_i\right]$ ставить у відповідність чіткому числу деяку нечітку множину, що містить набір кортежів, які

дорівнюють кількості функцій належності, що задані для лінгвістичної змінної.

Для спрощення запису введемо оператор *F*, який буде виконувати набір операцій: композиція, імплікація та агрегація. Результатом виконання над фазифікованим вектором вхідних змінних *x* оператора *F* буде множина

$$\tilde{y} = \frac{\mu_{d_1}(x^*)}{d_1} + \frac{\mu_{d_2}(x^*)}{d_2} + \cdots + \frac{\mu_{d_n}(x^*)}{d_n} \quad (2.19)$$

Для бази продукції з рисунку 2.2 виведемо:

$$\tilde{y}_1 = F\big(Fuzzy(x_1, x_2, x_3)\big), \quad (2.20)$$

$$\tilde{y}_2 = F\big(Fuzzy(x_4, x_5, x_6)\big), \quad (2.21)$$

$$\tilde{y}_3 = F\big(Fuzzy(x_7, x_8, x_9)\big), \quad (2.22)$$

$$\tilde{y}_4 = F\big(Fuzzy(y_1, y_2, y_3)\big) \text{ або } \tilde{y}_4 = F(\tilde{y}_1, \tilde{y}_2, \tilde{y}_3). \quad (2.23)$$

Якщо замінимо $\tilde{y}_1$, $\tilde{y}_2$ та $\tilde{y}_3$ у формулі (2.23), отримуємо:

$$\tilde{y}_4 = F\big(Fuzzy(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9)\big) \quad (2.24)$$

Результуюче значення виходу *y*, що відповідає вхідному вектору x^* визначається в результаті дефазифікації нечіткої множини $\tilde{y}$. Найбільш поширеним методом дефазифікації за Мамдані є метод центру ваги:

$$y = \frac{\int_{\underline{y}}^{\overline{y}} y \cdot \mu_{\tilde{y}}(y) dy}{\int_{\underline{y}}^{\overline{y}} \mu_{\tilde{y}}(y) dy}. \quad (2.25)$$

Дефазифікація, як операція обернена до фазифікації, буде позначена як:

$$y = deFuzzy(\tilde{y}). \quad (2.26)$$

Для більш узагальненого та компактнішого вигляду, введемо деякі позначення:

$l = \overline{1,k}$ – шар (level), де k – загальна кількість шарів. Для уточнення, шар – це структурна одиниця, де розміщені всі незалежні задачі, які можуть виконуватися паралельно, а результат виконання однієї задачі не впливає на обчислення інших задач.

$t_i = \overline{1, m_l}$ – задача (task) l-шару, де m_l – загальна кількість задач l-шару. Задача – це найменша розрахункова одиниця нечіткого логічного виводу. В даному випадку за схемою нечіткого логічного виводу за Мамдані.

x_i^{lt}, $i = \overline{1, n_{lt}}$ – змінні задачі t шару l. Змінна – це вхідна або вихідна (проміжна) лінгвістична змінна нечіткого виводу.

Будемо вважати, що запис $F_{i=1}^{k}$ позначає послідовне виконання k-разів оператора F згідно кількості шарів задачі.

Тоді для нечіткого виводу $\tilde{y}_{lt}$ отримуємо:

$$\tilde{y}_{lt} = F\left(Fuzzy\left(\left\{\tilde{y}_k^{lt}\right\}_{k=1}^{n}\right)\right). \quad (2.27)$$

За допомогою композиційного правила Заде отримуємо вираз:

$$\tilde{y}_{lt} = \left(\tilde{A}\left(\left\{x_i^{li}\right\}_{i=1}^{n}\right) \circ R^l(\tilde{y}_{i=1}^{t})\right). \quad (2.28)$$

В загальному вигляді можна отримати формулу:

$$\tilde{y} = F_{i=1}^{k}\left(F_{t_i=1}^{m_i}\left(F\left(Fuzzy\left(\left\{x_i^{li}\right\}_{i=1}^{n_d}\right)\right)\right)\right). \quad (2.29)$$

Після дефазифікації нечіткої множини отримуємо загальну формулу нечіткого логічного виводу наступного вигляду:

$$y = deFuzzy\left(F_{i=1}^{k}\left(F_{t_i=1}^{m_i}\left(F\left(Fuzzy\left(\left\{x_i^{li}\right\}_{i=1}^{n_d}\right)\right)\right)\right)\right). \quad (2.30)$$

Після використання правила Заде отримуємо:

$$\tilde{y} = \tilde{A}(\{x_i\}_{i=1}^{n}) \circ R^1(\tilde{y}_{i=1}^{t}). \quad (2.31)$$

2.4.3 Метод парних порівнянь

В рамках математичної моделі оцінки рівня КІБ організації запропоновано застосування методу парних порівнянь при визначенні векторів ваг питань $\{w_1^i, w_2^i, \dots, w_n^i\}$ та векторів ваг сукупності компетенцій $W = \{W_1, W_2, \dots, W_m\}$.

Для кожного набору компетенцій $C^i: Q^i \subset U_Q$ визначаються відповідні ваги питань, що відображають ціну відповідей. Для визначення ваг впливу на рівні, що знаходяться на наступному щаблі ієрархії, доцільно скористатися методом парних порівнянь. Даний метод є наочним та дає змогу визначити пріоритетність одних елементів над іншими, що робить його ефективним для встановлення ієрархії у багатокомпонентних моделях.

Суть методу полягає у висловлюванні експертом суджень стосовно оцінки пріоритетності одного елемента відносно іншого, що веде до створення матриці парних порівнянь. В основу суджень покладено фундаментальну шкалу оцінок Т. Сааті [101], адаптовану для наших потреб (Таблиця 2.1).

Таблиця 2.1 – Фундаментальна шкала абсолютних чисел

Величина важливості	Визначення	Пояснення
1	Рівна важливість	обидві субкомпетенції однаково впливають на формування компетенції
3	Помірна важливість одного над іншим	Досвід та судження трохи сприяють визначенню сильнішого впливу на результуючу компетенцію однієї субкомпетенції порівняно з іншою
5	Суттєва важливість	Досвід та судження сильно сприяють визначенню сильнішого впливу на результуючу компетенцію однієї субкомпетенції порівняно з іншою
7	Дуже сильна або продемонстрована важливість	Надається дуже сильна перевага визначенню сильнішого впливу на результуючу компетенцію однієї субкомпетенції порівняно з іншою; її домінування спостерігається на практиці
9	Надзвичайна важливість	Докази, що сприяють наданню переваги одній субкомпетенції перед іншою, є найвищим можливим порядком підтвердження
2, 4, 6, 8	Проміжні значення між двома суміжними судженнями	Коли потрібен компроміс
1,1…1,9	Додаткові значення за умов наближеної важливості	Може бути важко визначити найкраще значення, але порівняно з іншими контрастними діями розмір невеликих чисел не буде надто помітним, проте вони все ще можуть вказувати на відносну важливість субкомпетенції

Результатом парних порівнянь $Q^i = \left(q_{ij}^i\right)$ питань або сукупності компетенцій $C = c_{ij}$ є квадратна матриця. Невід'ємною властивістю є обернена симетричність отриманої матриці порівнянь, спираючись на те, що i-ий елемент по відношенню до j-го є оберненою величиною до значення оцінки щодо відношення j-го об'єкта до i-го, тобто:

$$w_{\text{j}}^i = \frac{1}{w_i^j}. \tag{2.32}$$

Таким чином, матриця парних порівнянь може мати наступний вигляд:

$$w = \begin{bmatrix} 1 & w_2^1 & w_3^1 & \dots & w_n^1 \\ \frac{1}{w_2^1} & 1 & \frac{1}{w_2^3} & \dots & w_n^2 \\ \frac{1}{w_3^1} & w_2^3 & 1 & \dots & \frac{1}{w_3^n} \\ \dots & \dots & \dots & 1 & \dots \\ \frac{1}{w_{\text{n}}^1} & \frac{1}{w_n^2} & w_3^n & \dots & 1 \end{bmatrix}. \tag{2.33}$$

Розташування обернених елементів матриці наведено в якості прикладу.

Наступною процедурою після заповнення матриці парних порівнянь є визначення середнього геометричного значення вектора цінностей α_i для кожного рядка матриці w, що матиме вигляд:

$$\alpha_i = \frac{\sqrt[n]{w_1^i \dots w_n^i}}{\sum_{i=1}^n \sqrt{w_1^i \dots w_n^i}}, i = \overline{1,n}. \tag{2.34}$$

Для отримання матриці ваг питань, яка в подальшому буде використана для формування ваги кожного питання, проведемо нормування отриманих значень α_i.

За умови великої кількості порівнюваних елементів можлива поява помилок при заповненні матриці порівнянь. Для їх виявлення застосовують індекс узгодженості

$$J_p = \frac{\lambda_{max} - n}{n-1}, \tag{2.35}$$

де λ_{max} – середнє арифметичне власного числа матриці w, що визначається як λ_{max} [102]. Чим ближче λ_{max} до n, тим точніше узгоджені відповіді експерта.

Таблиця 2.2 – Еталонні значення показника узгодженості [102]

Кількість об’єктів	3	4	5	6	7	8	9	10	11	12	13	14	15
J_p	0,58	0,9	1,12	1,24	1,32	1,41	1,45	1,49	1,51	1,54	1,56	1,57	1,59

За умови $J_p \leq 0{,}1J_e$ матрицю порівнянь вважають адекватною, а висновки експерта вірними.

2.4.4 Логіка антонімів

Для визначення набору ІБ-компетенцій, що мають бути наявні при виконанні певної ролі, ЛА пропонує ряд переваг, серед яких можливість створення моделі, що враховує взаємозв’язки між компонентами (ІБ-компетенціями), а також використання лінгвістичних оцінок із застосуванням математичного апарату. Докладніше аксіоматика ЛА висвітлена в роботах [103, 104].

Для побудови логічної моделі ІБ-компетенцій користувача [105, 106, 107] скористаємось основними положеннями ЛА [104]:

- Компетенції, що відображають деякі елементарні вимоги до КІБ користувача, позначаються через C_{ijk}.
- Властивість, протилежна C_{ijk}, позначається αC_{ijk}. Ці властивості утворюють антонімічні пари.
- C_{ijk} поставлені у відповідність числа $H\left(C_{ijk}\right)$, де H – символ функціоналу. Комбінацію $H(C_{ijk})$ слід розуміти як «ступінь наявності властивості (ІБ-компетенції) C_{ijk} в даному наборі (вимогах)».
- Взаємозв'язок антонімічної пари визначається як

$$H(\alpha C) = -log_2\left[1 - 2^{-H(C)}\right]. \quad (2.36)$$

- Графічна інтерпретація взаємозв’язку антонімічної пари приведена на рисунку 2.15. Ступінь присутності властивості C_i або протилежної αC_i визначається за допомогою набору модифікаторів – термів. При цьому

властивості C_i та αC_i – антоніми, а оцінки міри наявності $H(C_i)$ та $H(\alpha C_i)$ – синоніми [108].

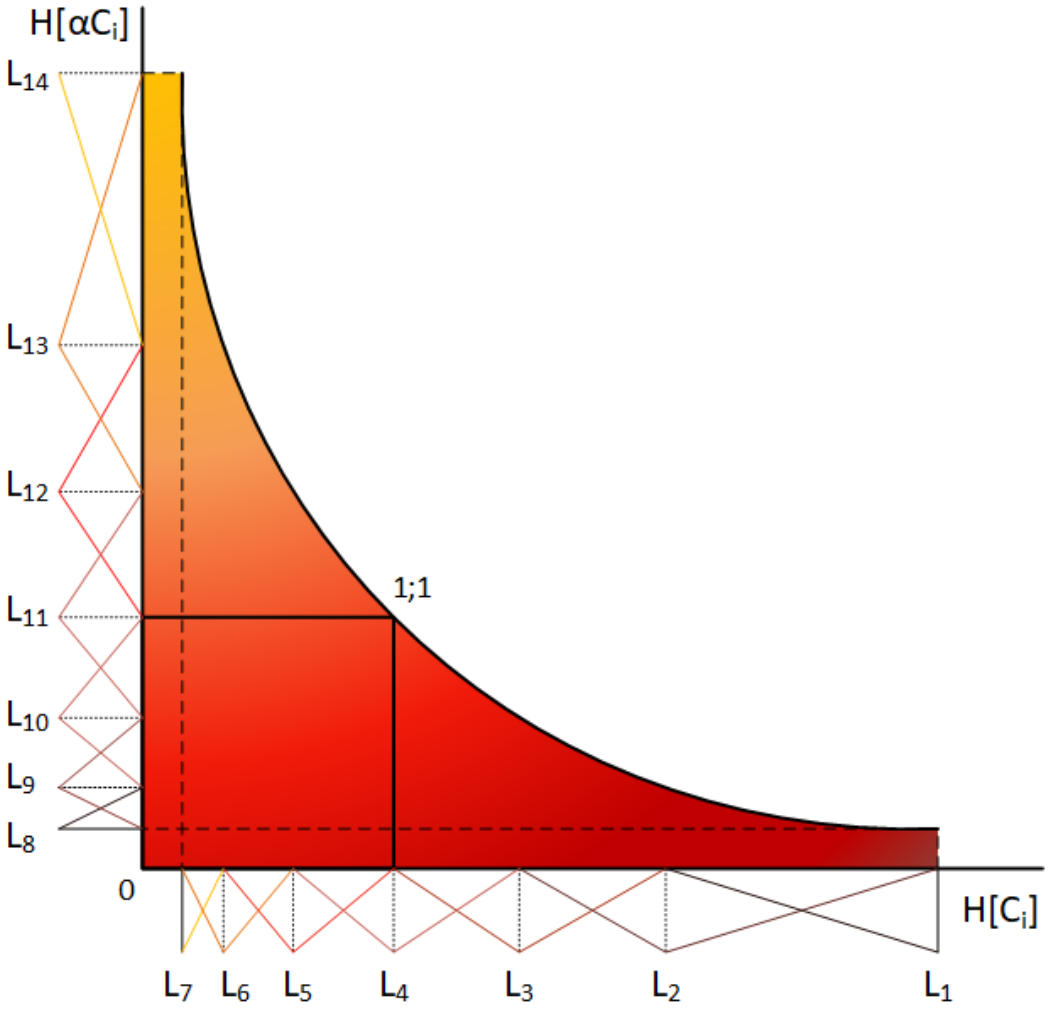

Рисунок 2.15 – Взаємозв'язок антонімічної пари C_i та αC_i

– Використовуються бінарні операції математичної логіки: β – аналогічно диз'юнкції («слабкий» зв'язок) і γ – аналогічно кон'юнкції («сильний» зв'язок):

$$\beta: \quad H(C_1 \beta C_2) = W_1 H(C_1) + W_2 H(C_2), \tag{2.37}$$

$$\gamma: \quad H(C_1 \gamma C_2) = -log_2\left[1 - (1 - 2^{-W_1 H(C_1)})(1 - 2^{-W_2 H(C_2)})\right], \tag{2.38}$$

– або

$$H(C_1 \gamma C_2) = -log_2\left[1 - \left(1 - 2^{-W_1 H(\alpha C_1) - W_2 H(\alpha C_2)}\right)\right], \tag{2.39}$$

– де W_1 і W_2 – вагові коефіцієнти, встановлені для властивостей (ІБ-компетенцій) C_1 і C_2.

Наведені залежності (2.37) – (2.38) можна інтерпретувати у наступному вигляді:

– оцінка $H(C_1 \beta C_2)$ комплексної властивості $C_1 \beta C_2$ приймає максимальне значення в разі максимальних значень оцінок $H(C_1)$ та $H(C_2)$. Якщо одна з властивостей нульова, оцінка $H(C_1 \beta C_2)$ не дорівнює нулю;
– оцінка $H(C_1 \gamma C_2)$ комплексної властивості $(C_1 \gamma C_2)$ набуває в разі максимальних значень оцінок $H(C_1)$ та $H(C_2)$. Проте якщо одна з властивостей дорівнює нулю, оцінка $H(C_1 \gamma C_2)$ наближається до нуля;
– $H(C_1 \gamma C_2) \leq H(C_1 \beta C_2)$, тобто оцінка сукупності властивостей при їх значній кореляції («сильний» зв'язок) завжди менше або дорівнює оцінці цих же властивостей при незначному («слабкому») взаємозв’язку.

Вихідними даними для створення математичної моделі оцінки ІБ-компетентності користувача є ієрархічна модель ІБ-компетенцій, інформація про взаємозв’язки між субкомпетенціями (складовими компонентами компетенцій), а також вагові коефіцієнти W. Зазначимо, що кожна посада містить унікальний набір ІБ-компетенцій, що заздалегідь визначені експертом. Взаємозв’язки між субкомпетенціями можна інтерпретувати наступним чином: «сильний» зв’язок відображається як послідовне поєднання елементів, тоді як «слабкий» зв’язок представлений паралельним розташуванням субкомпетенцій.

ІБ-компетентність користувача (співробітника) можна представити як багатокомпонентну систему ІБ-компетенцій, що визначають здатність користувача здійснювати безпечну професійну діяльність в рамках його посади. Залежно від посади (а також набору ролей, що їх виконує співробітник в різній мірі) ієрархічна модель ІБ-компетенцій буде представляти собою унікальну комбінацію ІБ-компетенцій (субкомпетенцій).

Отже, умовно згрупуємо ІБ-компетенції у дві групи: технічні та персональні. Під технічними ІБ-компетенціями будемо розуміти такі компетенції, що стосуються питань впровадження та налаштування СЗІБ, її

апаратної складової, адміністрування та інших робіт. Під персональними ІБ-компетенціями будемо мати на увазі знання, уміння та досвід, що пов'язані з «м'якими навичками» (так звані soft skills), взаємодію із внутрішнім та зовнішнім інформаційними середовищами, обізнаність щодо загроз, реалізація яких пов'язана з людським фактором, та ін.

Логічна модель ІБ-компетенцій співробітника представлена на рисунку 2.16.

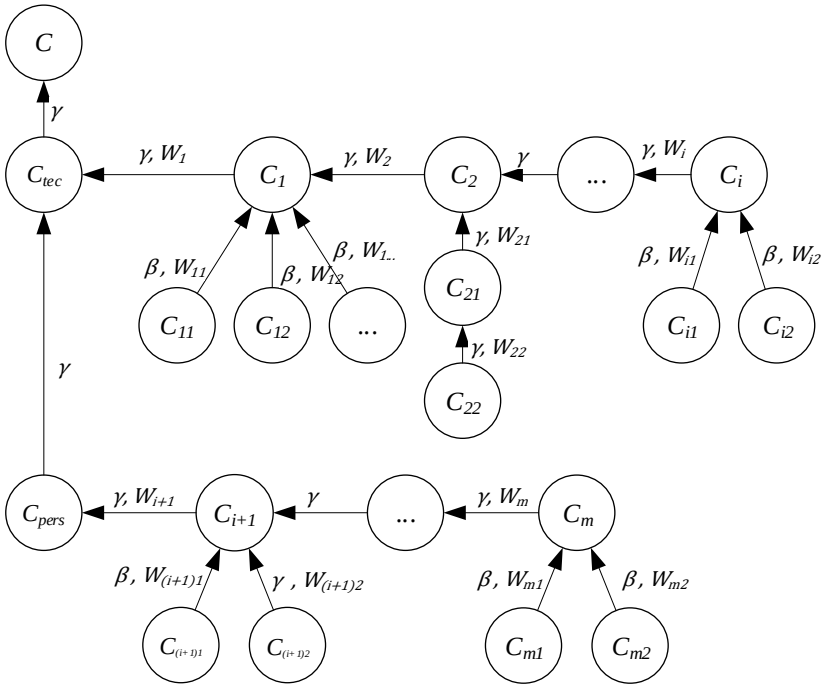

Рисунок 2.16 – Логічна модель ІБ-компетентності користувача

Інтегральна оцінка ІБ-компетентності користувача матиме вигляд:

$$H(C) = H\left(C_{tec}\gamma C_{pers}\right), \tag{2.40}$$

тобто

$$H(C) = -log_2\left[1 - \left(1 - 2^{-H(C_{tec})}\right)\left(1 - 2^{-H\left(C_{pers}\right)}\right)\right]. \tag{2.41}$$

Для складових C_{tec} та C_{pers}

$$H(C_{tec}) = -log_2\left[1 - \prod_1^i\left(1 - 2^{-W_i H(C_i)}\right)\right], \tag{2.42}$$

$$H\left(C_{pers}\right) = -log_2\left[1 - \prod_{k=i+1}^m\left(1 - 2^{-W_k H(C_k)}\right)\right]. \tag{2.43}$$

Варіанти визначення повноти ІБ-компетенцій на нижчому рівні представлені у вигляді залежностей (2.44) – (2.47):

$$H(C_1) = \sum W_{1i} H(C_{1i}), \quad (2.44)$$

$$H(C_2) = -log_2\left[1 - \left(1 - 2^{-W_{21}H(C_{21})}\right)\left(1 - 2^{-W_{22}H(C_{22})}\right)\right], \quad (2.45)$$

$$H(C_i) = W_{i1} H(C_{i2}) + W_{i2} H(C_{i2}), \quad (2.46)$$

$$H(C_{i+1}) = -log_2\left[1 - 2^{-W_{(i+1)1}H\left(C_{(i+1)2}\right)}\right] + W_{(i+1)2} H\left(C_{(i+1)2}\right). \quad (2.47)$$

Таким чином, математичне представлення логічної моделі оцінки ІБ-компетенцій користувача буде мати унікальний вигляд залежно від рішення експерта щодо набору ІБ-компетенцій, вагових коефіцієнтів та типу зв'язків.

2.5 Механізм отримання висновку про рівень КІБ та рекомендацій заходів для його покращення

Аналіз параметрів КІБ та їх індикаторів, що були розглянуті в п.1.3, дозволяє сформулювати СНВ. Для побудови СНВ, як і у випадку обробки результатів опитувань, використано пакет Fuzzy Logic Designer обчислювального середовища MATLAB. Переваги ієрархічного підходу, згадані раніше, роблять його застосування доцільним та зручним і для створення багаторівневої моделі для НЛВ. Вхідні, проміжні та вихідні лінгвістичні змінні, їх позначення, тип функцій належності та набори термів наведені в Додатку В.

Взаємозв'язки між індикаторами ІБ можна представити у вигляді ієрархічної нечіткої моделі, яка наведена на рисунку 2.17.

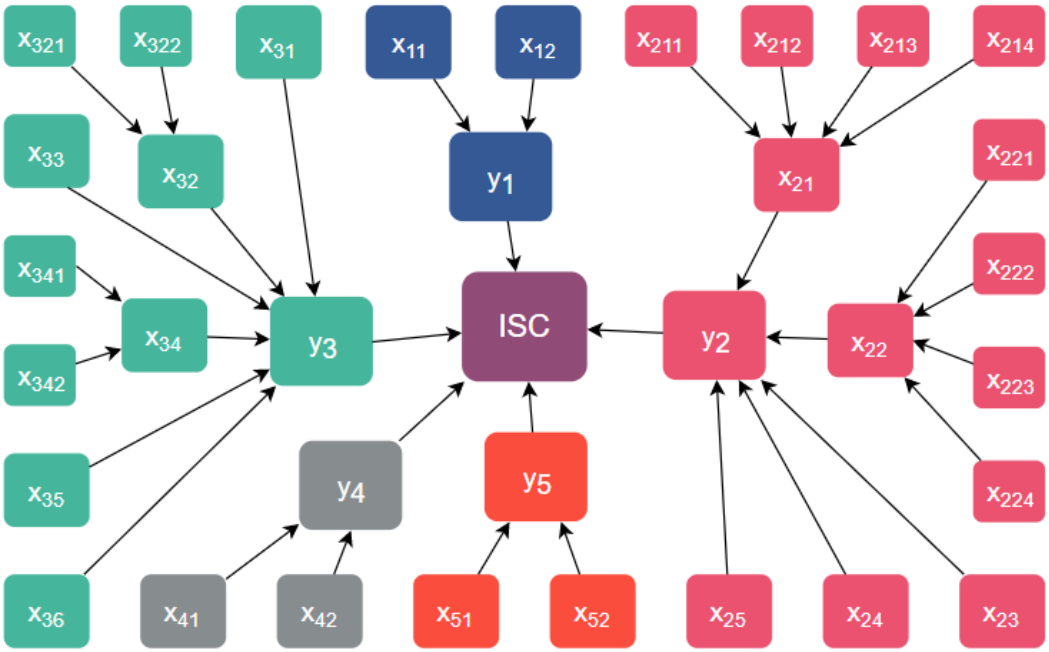

Рисунок 2.17 – Mind-map оцінювання рівня КІБ організації

Загальний рівень КІБ організації можна визначити як:

$$ISC = f(y_1, y_2, y_3, y_4, y_5), \quad (2.48)$$

де y_1 – рівень ІБ-компетенції працівників;

y_2 – позиція адміністрації та підтримка КІБ;

y_3 – контроль над діями, що пов'язані з ІБ;

y_4 – комунікації;

y_5 – емоційний клімат.

СНВ основних показників рівня КІБ організації можна визначити за наступними залежностями:

- рівень ІБ-компетенції працівників:

$$y_1 = f(x_{11}, x_{12}, x_{13}). \quad (2.49)$$

- позиція адміністрації та підтримка КІБ:

$$y_2 = f(x_{21}, x_{22}, x_{23}, x_{24}, x_{25}), \quad (2.50)$$

де

$$x_{21} = f(x_{211}, x_{212}, x_{213}, x_{214}), \quad (2.51)$$

$$x_{22} = f(x_{221}, x_{222}, x_{223}, x_{224}, x_{225}, x_{226}). \quad (2.52)$$

- контроль над діями, що пов'язані з ІБ:

$$y_3 = f(x_{31}, x_{32}, x_{33}, x_{34}, x_{35}, x_{36}), \quad (2.53)$$

де

$$x_{32} = f(x_{321}, x_{322}), \quad (2.54)$$

$$x_{34} = f(x_{341}, x_{342}). \quad (2.55)$$

– комунікації:

$$y_4 = f(x_{41}, x_{42}). \quad (2.56)$$

– емоційний клімат:

$$y_5 = f(x_{51}, x_{52}). \quad (2.57)$$

Змінна «рівень КІБ організації» ISC характеризується набором термів {початковий, фрагментарний, системний, керований, управління КІБ}, що відповідає моделі зрілості СЗІБ за стандартом NIST.

Результатом оцінювання поточної ситуації, окрім відомості про рівень КІБ, має бути і визначений набір рекомендацій, що повинні відповідати заходам з підвищення поточного рівня КІБ організації, то СНВ повинна відповідати MIMO[4]-типу. Тож виходячи з результатів опитувань та анкетування, а також приймаючи до уваги їх співставлення з відповідними вимогами, СНВ продукує дві вихідні змінні. Перша вказує на визначений рівень КІБ організації, друга – заходи, які мають бути проведені для задоволення вимог.

2.6 Модель повномасштабного впровадження культури інформаційної безпеки

Культура інформаційної безпеки, будучи за своєю природою невід'ємною частиною корпоративної культури, є складною динамічною системою. З іншого боку, інформаційний простір організації є частиною штучно створеного середовища в результаті інформаційно-виробничої діяльності колективу організації та зовнішнього інформаційного простору.

[4] Multiple Inputs – Multiple Outputs

І кожен учасник цього процесу впливає на стан безпеки бізнес-процесів, які нерозривно пов’язані з інформаційними активами організації.

Залежно від ресурсів організації, її можливостей та цілей проведення аудиту ІБ, на практиці допускаються такі методи оцінки: еталонна оцінка, оцінка загальних витрат та ризик-орієнтована оцінка [109]. Кожен з методів має свої переваги, але для оцінки КІБ організації з позиції учасників інформаційних процесів оцінка на основі ризику є майже єдиним варіантом.

Ризик-оцінка ІБ організації – це спосіб оцінки ризиків ІБ, що виникають в інформаційному просторі організації, порівняння існуючих ризиків ІБ та вжитих заходів щодо їх подолання. Як результат, слід оцінити здатність організації ефективно управляти ІБ-ризиками для досягнення своїх цілей.

Управління КІБ, як управління організаційною культурою загалом, можливе лише за умови ретельного, глибокого та тривалого процесу розробки, оцінки та інтегрованого застосування позитивних управлінських рішень. Формування ефективної корпоративної культури – складний і тривалий процес, що вимагає критичної оцінки та постійного вдосконалення.

Таким чином, в разі виникнення проблеми з визначенням, формуванням та подальшим вдосконаленням КІБ працівників та учасників інформаційних процесів організації шляхом підвищення обізнаності в галузі ІБ, для впровадження КІБ в соціально-технологічну культуру може бути використаний комплексний проектний підхід. Основними етапами можуть бути:

- обґрунтування доцільності та необхідності впровадження або вдосконалення КІБ організації;
- аналіз поточного рівня КІБ в організації, та планування заходів щодо її впровадження або покращення;
- реалізація запланованих заходів та впровадження КІБ для всіх учасників інформаційних процесів організації.

Питання формування та масштабного впровадження КІБ в організаціях сьогодні повинне розглядатися як стандартизована процедура. Зрозуміло, що

впровадження КІБ необхідно реалізовувати за допомогою проектного підходу та з врахуванням необхідності постійного поліпшення виконання даного процесу. Графічна модель, що представлена на рисунку 2.18, передбачає проектний та процесний підходи для формування, впровадження та реалізації КІБ [110].

На першому етапі здійснюється вибір об’єкта впровадження. В практиці управління рекомендовано впроваджувати зміни спочатку в рамках одного підрозділу, для визначення помилок процесу та їх усунення без значних втрат. Це може бути будь-який підрозділ в організації, що має найбільшу потребу в таких змінах, або підрозділ, який проявляє найбільшу здатність до змін. В такому підрозділі процес проходитиме з меншими зусиллями та подолання супротиву змінам та витратами на навчання. В результаті етапу повинна бути сформована команда зі спеціалістів підрозділу, в якому буде впроваджуватися або поліпшуватися КІБ, яка буде впроваджувати зміни. Ця команда повинна визначити цілі та задачі даних змін.

Здійснення оцінки існуючого рівня КІБ на обраному об’єкті можна проводити різними відомими методами (метод оцінки ризиків, методи оцінки за еталоном або вартісними показниками). В результаті, якщо рівень дуже високий, то варто обрати інший підрозділ. При низькій оцінці приймаємо рішення щодо розробки проекту впровадження КІБ. Якщо ж існуючий рівень є середнім, або вище середнього можна проводити покращення цього рівня. Крім визначення остаточних оцінок даний процес також створить базу для подальшого визначення ефективності впровадження змін за допомогою порівняння поточних показників із одержаними в результаті.

Далі, в залежності від рівня КІБ в обраному об’єкті, застосовуємо проектний або процесний підходи. В першому випадку команда займається розробкою проекту з впровадження КІБ в обраному підрозділі. Тут використовуються відомі методології управління проектами, які повинні забезпечити впровадження змін у визначений термін, в рамках бюджету та встановленого рівня якості. Другий підхід містить розробку заходів щодо

покращення існуючої системи КІБ та проведення стандартизації процедури після впровадження таких заходів. Процес стандартизації дозволяє визначати межі процесів, а також гарантує, що кожен буде розуміти та виконувати оновлений процес відповідним чином. В результаті з'являється детальна документована процедура (методика), яка описує не тільки кращий процес підтримки КІБ, а є засобом для недопущення минулих помилок.

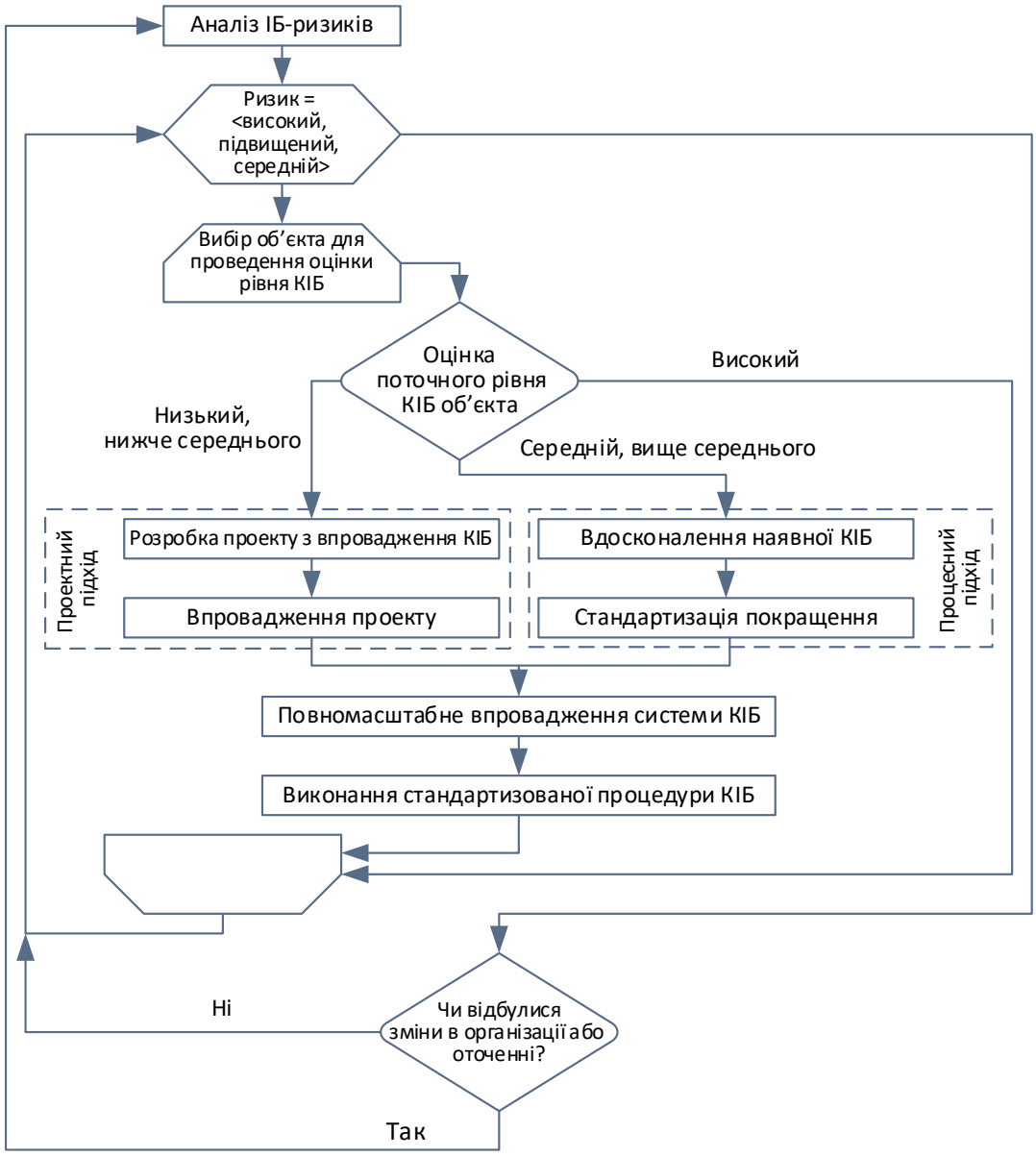

Рисунок 2.18 – Графічна модель забезпечення КІБ в організації

Наступний етап – повномасштабна реалізація проекту впровадження КІБ в організації та виконання стандартизованої процедури. Тут

рекомендується використовувати цикл забезпечення якості Standardize-Do-Check-Act (SDCA) Демінга [111, 112]. При цьому необхідно стандартизувати процедури КІБ на рівні всієї організації, провести перепідготовку або навчання персоналу, вимагати чіткого виконання стандартизованої процедури (рисунок 2.19). Дуже великою цінністю на даному етапі є досвід персоналу та наявність розробленої документації, які дозволяють перейти на наступний рівень управління КІБ в організації, і забезпечити більш високу ефективність реалізації процесу постійного покращення системи КІБ.

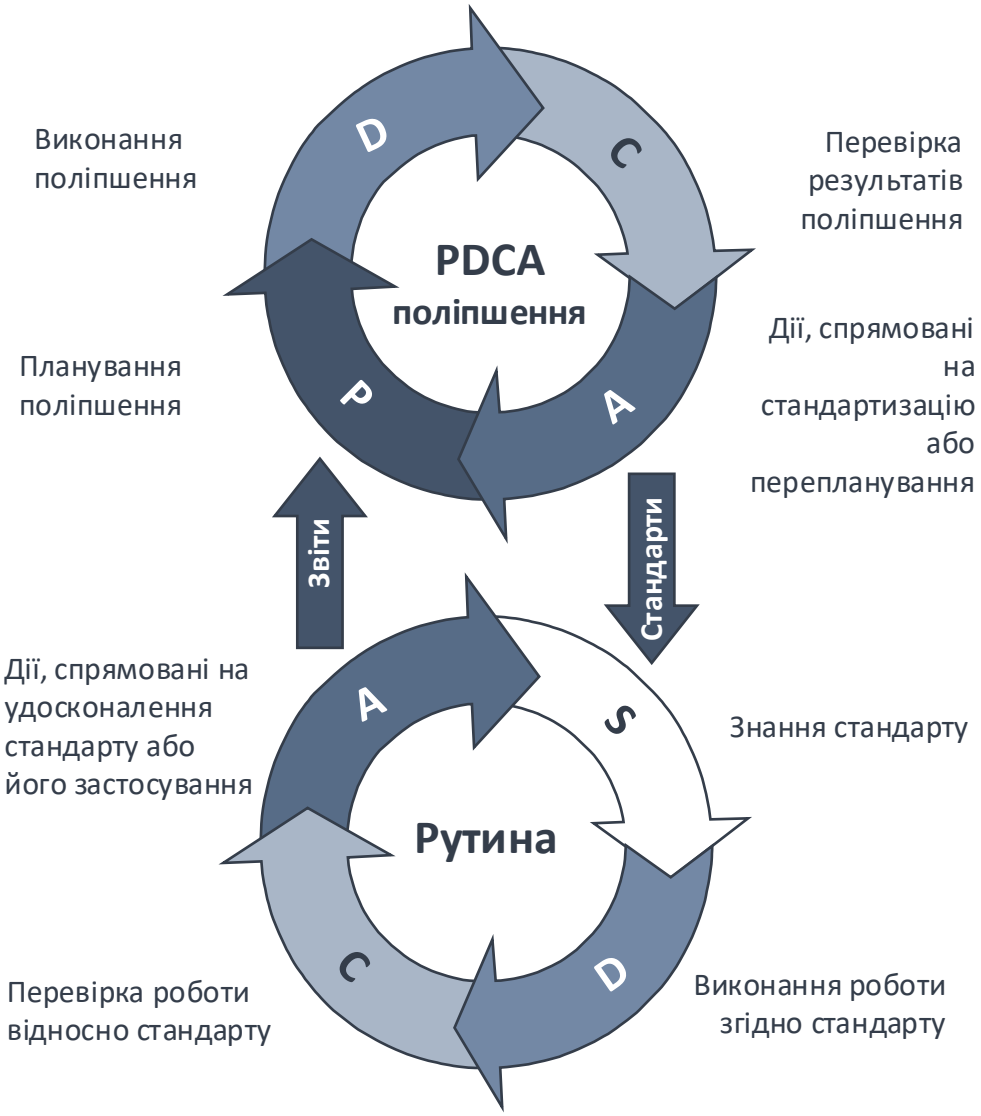

Рисунок 2.19 – Використання циклів PDCA-SDCA за процесного підходу

Застосування проектного підходу у випадку виявлення низького рівня КІБ, особливо коли це є критичним фактором, дозволяє інтенсифікувати заходи з поліпшення поточного стану КІБ та закріплення надбань в даному напрямку.

Успіх впроваджених заходів буде залежати від відстежування змін в організації та оточуючому середовищі. Використання запропонованої моделі є ключовим елементом для вчасного та ефективного реагування на такі зміни для забезпечення ефективної взаємодії як всередині організації так із зовнішнім світом.

Висновки до розділу 2

1) Запропонована модель визначення вимог до рівня КІБ працівників враховує роль співробітника у загальній системі інформаційної безпеки організації та пов’язані з нею ІБ-ризики. Вона містить технічні та персональні аспекти людино-машинної взаємодії та враховує ризики, пов’язані з професійною діяльністю.
2) Визначені вимоги до персональної КІБ співробітників різних організаційних рівнів та їх оцінка, покладені в основу моделі оцінки рівня КІБ організації. Запропонована модель може бути використана як для оцінки поточної ситуації з наданням рекомендацій щодо заходів посилення КІБ, так і для отримання пропозицій щодо можливих посад під час оцінки кандидатів.
3) Розроблена модель системи інтегральної оцінки рівня КІБ організації враховує розмежування вимог до компетентності в галузі ІБ залежно від ролі, яку співробітники відіграють у загальній системі ІБ організації. Перехід від якісних до кількісних показників здійснюється шляхом використання методів нечіткої логіки. Такі перетворення можуть відбуватися на останніх трьох рівнях оцінювання, в залежності від того, в якій формі (якісній або кількісній) бажано отримати показники. Інтегральний показник

рівня КІБ персоналу можна використовувати при проведенні аудиту системи забезпечення ІБ організації, а також при оцінюванні ефективності впровадження заходів для її розвитку та вдосконалення.

4) Модель, запропонована для повномасштабної реалізації КІБ організації, визначає різні підходи з урахуванням специфіки організації. Вона може бути застосована при розробці автоматизованих систем управління КІБ на різних рівнях.

В якості набору основних рекомендацій щодо забезпечення відповідного рівня КІБ організації пропонується розробити інформаційну систему, яка визначатиме рівень існуючої КІБ організації, включаючи оцінку рівня персональної КІБ.

Результати досліджень, приведених в розділі, опубліковані в роботах [72, 90-92, 105-107, 110].

РОЗДІЛ 3
БІЗНЕС-ЛОГІКА ВИЗНАЧЕННЯ РІВНЯ КУЛЬТУРИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ ТА РОЗРОБКА ІНФОРМАЦІЙНОЇ СИСТЕМИ

3.1 Бізнес-логіка визначення рівня культури інформаційної безпеки організації

3.1.1 Загальна функціональна модель

Концептуальна модель бізнес-процесу «Визначити рівень КІБ організації» [114] представлена на рисунку 3.1.

Рисунок 3.1 – Функціональна модель бізнес-процесу верхнього рівня «Визначити рівень КІБ організації»

Вхідною інформацією для системи є: перелік ролей, компетенцій, тем, питань, потенційні ситуаційні рекомендації та аналіз ІБ-ризиків організації. Ці дані є обов’язковими для початку роботи. Керуючими елементами системи є нормативна документація та міжнародні стандарти в ІБ-галузі (стандарти сімейства ISO/IEC 27000), сфера діяльності організації та її потреби, вимоги внутрішньої ІБ-політики, штатний розпис, посадові інструкції, а також професійні стандарти, що містять набір компетенцій. В ролі механізмів керування виступає експерт в галузі інформаційної безпеки організацій (в його

обов’язки входить наповнення БД вхідною інформацією, визначення вагових коефіцієнтів, формування анкет, їх поширення та збір зворотної інформації, створення БП нечітких моделей, перевірка звіту та рекомендацій), хмарні сервіси для поширення анкет та збору відповідей, програмне забезпечення як інструмент, який використовують в роботі системи всі учасники процесу, база даних (БД) для зберігання інформації, логіка антонімів (при формуванні матриці компетенцій), метод парних порівнянь (при визначенні вагових коефіцієнтів питань в межах анкети), методи нечіткої логіки (для оцінки персонального рівня КІБ співробітників), нечітка кластеризація (для створення кластерів питань за темами), математичні моделі оцінки КІБ відділу та організації. На виході система повинна надати звіт про проведене оцінювання рівня КІБ організації та рекомендації що до покращення цього рівня.

3.1.1.1 Вхідна інформація

Перелік тем визначають аспекти, що пов’язані з трудовою діяльністю співробітників як користувачів внутрішнього інформаційного простору. Перелік тем формується експертом на основі знань у даній предметній області.

Перелік ролей. В рамках виконання посадових обов’язків співробітник може виконувати декілька ролей у різному обсязі. Так, наприклад, обов’язки оператора можуть бути доповнені деякими базовими вимогами з адміністрування робочого ПК окрім внесення даних в де-яку інформаційну систему. Джерелом переліку ролей є штатний розпис організації та комплект посадових інструкцій.

Перелік питань. Для формування анкет експерт наповнює БД коректно сформованими питаннями та варіантами відповідей, що будуть запропоновані респондентам для вибору.

Перелік компетенцій. Джерелом переліку компетенцій є професійний стандарт, вимоги або потреби організації, посадові інструкції, внутрішня політика ІБ організації, тощо. Перелік компетенцій слугує для визначення міри наявності або повноти відповідних компетенцій у користувача внутрішнього

інформаційного середовища (співробітника) згідно ролей, що він виконує в рамках посади.

Потенційні ситуаційні рекомендації. Перелік рекомендованих (приписаних) дій, що являються наслідком збігу несприятливих оцінок за певними критеріями оцінки персональної КІБ.

Аналіз ІБ-ризиків організації покладений в основу формування вимог до рівня КІБ організації, визначає аспекти, що потребують посилення через поглиблення знань для ведення успішної бізнес-діяльності організації. Ризик-аналіз дозволяє виділити вразливі елементи системи (ПЗ, процеси, учасники) та підготувати вимоги, що висуваються до персональної КІБ, за підрозділами та організації в цілому.

3.1.1.2 Керуючі елементи системи

Нормативна документація – законодавча база України, що складається з набору законодавчих, нормативно-правових та нормативних актів щодо інформаційної безпеки в Україні.

В основу покладені ЗУ «Про інформацію» від 02.10.1992 №2657-XII [2], «Про захист персональних даних» від 01 червня 2010 №2297-VI [115], «Про основні засади забезпечення кібербезпеки України» [116], «Про захист інформації в інформаційно-телекомунікаційних системах» [117], «Про електронні документи та електронний документообіг» [118] та ін., а також нормативні документи, постанови Кабінету Міністрів України, та ін.

Згідно ГСТУ СУІБ 2.0/ISO/IEC 27002:2010 «Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою» [119], формування вимог до ІБ здійснюється на базі трьох основних джерел:

- Оцінка ризиків для організації на основі бізнес-стратегії організації. Результатом ІБ-ризик аналізу є перелік ідентифікованих загроз та оцінка вразливості та потенційних наслідків.
- Правові вимоги, що діють на підставі закону, договірні умови з партнерами та підрядниками; соціально-культурне середовище.

– Внутрішня політика організації в галузі ІБ, що регламентує процедури обробки та виробництва інформації у внутрішньому інформаційному просторі.

Міжнародні стандарти групи ISO/IEC 2700X (такі як ISO/IEC 27001, 27002, 27032 та ін.) використовуються в якості найкращих практик; слугують джерелом рекомендацій щодо покращення наявної ситуації.

Штатний розпис – джерело наповнення переліку посад і пов'язаних з ними ролей. Штатний розпис є обов'язковим документом для організації.

Сфера діяльності організації визначає і вимоги, і тематику, що в подальшому використовуються для формування анкет.

Професійні стандарти є основою для формування матриці компетенцій. Також слід звернути увагу на ті виробничі потреби, що супроводжують діяльність організації. Якщо умови внутрішньої ІБ-політики не дозволяють виконання визначених бізнес-процесів шляхом спрямування на аутсорсінг, такі бізнес-процеси мають бути забезпечені кваліфікованими та вузькоспеціалізованими фахівцями з певної галузі, що мають володіти унікальними компетенціями.

3.1.1.3 Елементи і механізми виконання

Експерт є носієм глибоких специфічних знань та практичного досвіду в галузі ІБ організації. Експерт (або група експертів) приймає участь у кожному етапі оцінки КІБ організації.

Першочерговими функціями експерту є наповнення таблиць БД системи первинною інформацією (формування вимог до ІБ; наповнення БД типових ситуаційних рекомендацій (заходів), спрямованих на підвищення рівня КІБ співробітників та організації; створення переліку питань для анкетування та їх розподіл за темами; формування переліку ролей (на базі посад зі штатного розпису); наповнення матриці компетенцій).

На другому етапі експерт призначає вагові коефіцієнти, що відображають ступінь належності питань до набору тем, вагу кожного питання (впливу на результуючу оцінку анкетування); встановлення впливу ролей на

загальний рівень КІБ підрозділу; призначення ваг компетенцій в рамках кожної ролі. Експерт формує базу правил (БП) для нечіткої моделі оцінки рівня персональної КІБ співробітників, а також БП визначення рекомендацій.

Також на завершальному етапі експерт перевіряє коректність отриманого звіту та набору рекомендацій для підсилення рівня КІБ організації через впровадження заходів з підвищення обізнаності та практичного досвіду працівників (підвищення персональної КІБ).

Програмне забезпечення (ПЗ). Програмне забезпечення складається з 6 модулів, кожен з яких задіяний на різних етапах ІБ-аудиту організації. Коротко їх можна описати як модуль збору даних, модуль генерації анкет, модуль проведення анкетування, модулі оцінки рівня КІБ підрозділу та організації, а також модуль комплексної оцінки. Детальніше архітектура ПЗ наведена в підрозділі 3.4.

База даних. Для реалізації системи оцінки КІБ організації використовується єдина БД, а не сукупність модульних БД. Вона містить інформацію про такі основні сутності, як відомості про користувачів, питання для анкетування, вимоги та ін. Детальніше діаграма сутностей розглянута в підрозділі 3.5.

Логіка антонімів. Під час наповнення інформаційної системи вхідною інформацією логіка антонімів використовується при формуванні матриці компетенцій з переліку компетенцій. Використання ЛА дозволяє вказати тип зв’язків (сильні або слабкі) між компетенціями, що мають бути наявні у кваліфікованого фахівця при виконанні набору ролей в рамках обов’язків за певною посадою.

Нечітка кластеризація використовується при формуванні кластерів питань за темами за відповідною матрицею ступенів належності для подальшої генерації анкет.

Методи нечіткої логіки (НЛ). На основі лінгвістичних оцінок рівень персональної КІБ респондента визначається за допомогою нечіткої моделі оцінки, тобто за допомогою нечіткої логіки. Подальша дефазифікація

результату анкетування передається на вхід до математичної моделі оцінки КІБ підрозділу.

Метод парних порівнянь є основою для призначення ваг впливу кожного питання на результуючу оцінку анкети. Ці величини встановлюються експертом на основі створеної матриці парних порівнянь.

Хмарні сервіси. Анкетування проводиться в режимі онлайн за допомогою анкет-форм, що створені та поширюються за підтримки хмарних сервісів (Google Forms, Microsoft Forms, Visual Paradigm Forms, тощо). Такий підхід має наступні переваги: вільний доступ, не потребує спеціалізованих знань з розробки, забезпечує автоматизований збір відповідей у таблиці (Google Sheet, Microsoft Excel, Visual Paradigm Form Results, тощо), можливість завантаження до БД інформаційної системи оцінки рівня КІБ організації.

Математична модель оцінки КІБ підрозділу, що описана в п. 2.3, визначає рівень КІБ підрозділу на основі персональних оцінок його співробітників з врахуванням матриці ваг ролей, що відповідають посадам респондентів.

Математична модель оцінки КІБ організації визначає механізм визначення загального рівня КІБ організації на базі результатів оцінок КІБ за структурними підрозділами, що отримані на попередньому етапі. Дана модель описана в п. 2.3.

3.1.1.4 Вихідна інформація

Інформаційна система оцінки рівня КІБ організації має виконувати дві головні функції: оцінка наявного рівня КІБ організації на базі персональних оцінок співробітників організації, результати якої мають бути представлені у вигляді звіту; у випадку невідповідності рівневі, що визначений вимогами до ІБ, звіт має містити набір рекомендацій щодо заходів, спрямованих на підвищення рівня КІБ співробітників та організації.

Вихідною інформацією для інформаційної системи оцінки рівня КІБ організації є звіт про оцінку наявного рівня КІБ організації та рекомендації

щодо підвищення рівня КІБ організації у випадку невідповідності показників вимогам до КІБ організації.

Звіт – це документ, що генерується системою як результат діяльності, спрямованої на визначення рівня КІБ організації, спираючись на оцінки КІБ персоналу з врахуванням вимог до ІБ організації, посадовими обов'язками, що визначають компетенції в ІБ-галузі.

Рекомендації. У випадку виявлення недостатнього рівня наявної КІБ, система надає відповідні рекомендації, що мають носити персональний характер, надають пояснення та директиви (поради) щодо усунення прогалин у теоретичній та/або практичній підготовці, набуття додаткового досвіду з метою доповнення ІБ-компетентності користувачів внутрішнього інформаційного простору – співробітників та керівників організації.

Рекомендації можуть містити посилання на тематичний матеріал, семінари, вебінари, курси, статті та інші навчальні матеріали.

3.1.2 Функціональна модель бізнес-процесу другого рівня

В результаті декомпозиції загальної задачі «Визначити рівень КІБ організації» (рисунок 3.2) процес поділено на 6 основних робіт:

1) Наповнити систему вхідною інформацією;
2) Згенерувати анкети;
3) Провести анкетування;
4) Оцінити КІБ за структурними підрозділами;
5) Оцінити рівень КІБ організації;
6) Створити звіт та надати рекомендації.

Перш ніж проводити оцінювання рівня КІБ організації, експерт за допомогою програмного забезпечення повинен наповнити систему необхідною інформацією за допомогою модулю збору даних. На рисунку 3.2 наочно представлено етапи, а також керуючі елементи та механізми, що залучені на відповідному етапі. Зібрана початкова інформація зберігається в БД, та використовується для генерування анкет. Приймаючи до уваги, що

завдяки сфері діяльності та місії кожна організація має унікальні риси, може відрізнятися за структурою, експерт має генерувати окремі набори анкет, які будуть зберігатися в базі даних. Після збору всієї інформації, її структуруванню та заповнення вагових матриць, а також генерації анкет система готова до проведення оцінки рівня КІБ організації.

Використовуючи хмарні сервіси, кожному працівникові організації надається електронна форма-анкета для проведення опитування. Після завершення опитування всі відповіді працівників використовуються для проведення оцінювання КІБ по кожному структурному підрозділу організації окремо. На основі отриманих результатів по підрозділах проводиться визначення рівня КІБ всієї організації в цілому. Фінальним етапом є генерація звіту про результати оцінювання, та надання організації рекомендації щодо вибору заходів з підвищення рівня КІБ.

3.1.3 Функціональна модель бізнес-процесу третього рівня

3.1.3.1 IDEF0 1-го етапу оцінки КІБ організації

Розглянемо кожен з етапів оцінки детальніше.

На першому етапі експерт виконує наступні завдання (рисунок 3.3):

- Сформувати вимоги до рівня КІБ організації. Згідно положень нормативної документації, вимог внутрішньої політики ІБ організації, а також найкращих практик міжнародних стандартів групи ISO/IEC 27000, на основі аналізу ІБ-ризиків організації експерт формує вимоги до рівня КІБ організації за певними показниками. Отримані вимоги до рівня КІБ організації зберігаються в БД.
- Заповнити БД ситуаційних рекомендацій щодо підвищення рівня КІБ (персонально, на рівні підрозділу, організації). Експерт, маючи знання про можливі заходи з підвищення рівня КІБ, формує ситуаційні рекомендації, що мають бути збережені у відповідній таблиці БД.

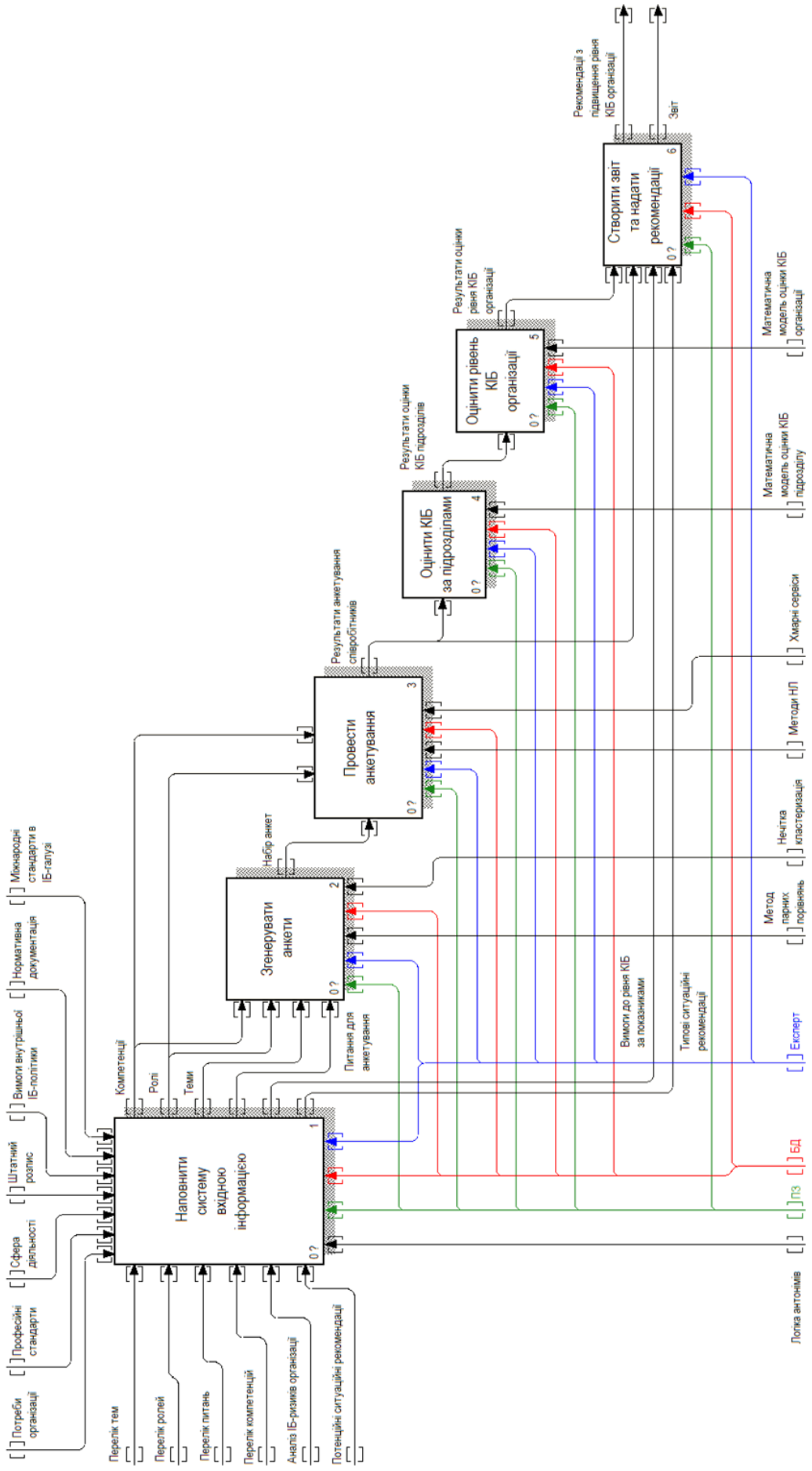

Рисунок 3.2 – Функціональна модель бізнес-процесу другого рівня «Визначити рівень КІБ організації»

- Створити множину питань в галузі ІБ. Під час створення переліку питань, що будуть використані при генерації анкет, експерт має керуватися нормативною документацією, міжнародними стандартами в ІБ-галузі (насамперед ISO/IEC 27001, 27002) та вимогами ІБ-політики, що діють всередині організації. Відібрані та відредаговані питання, а також варіанти відповідей заносяться до відповідних таблиць БД.
- Створити та відредагувати теми. Теми мають бути сформовані, виходячи зі сфери діяльності організації. Вони можуть стосуватися технічних і технологічних аспектів, взаємодії із зовнішнім інформаційним простором та його учасниками, іншими аспектами діяльності, що прямо або опосередковано впливають на КІБ. Відібрані та відредаговані теми заносяться до таблиці БД.
- Сформувати перелік ролей. Перелік ролей наповнюється експертом на основі штатного розпису організації та посадових інструкцій. Набір ролей зберігається в таблиці БД.
- Сформувати матрицю компетенцій в галузі ІБ. Перелік компетенцій, що є обов’язковою вхідною інформацією, має бути відредагований експертом, спираючись на професійні стандарти та власні потреби організації. Прийняття рішення про включення певної компетенції до матриці здійснюється на базі логіки антонімів. Відібрані компетенції заносяться експертом до таблиці БД.

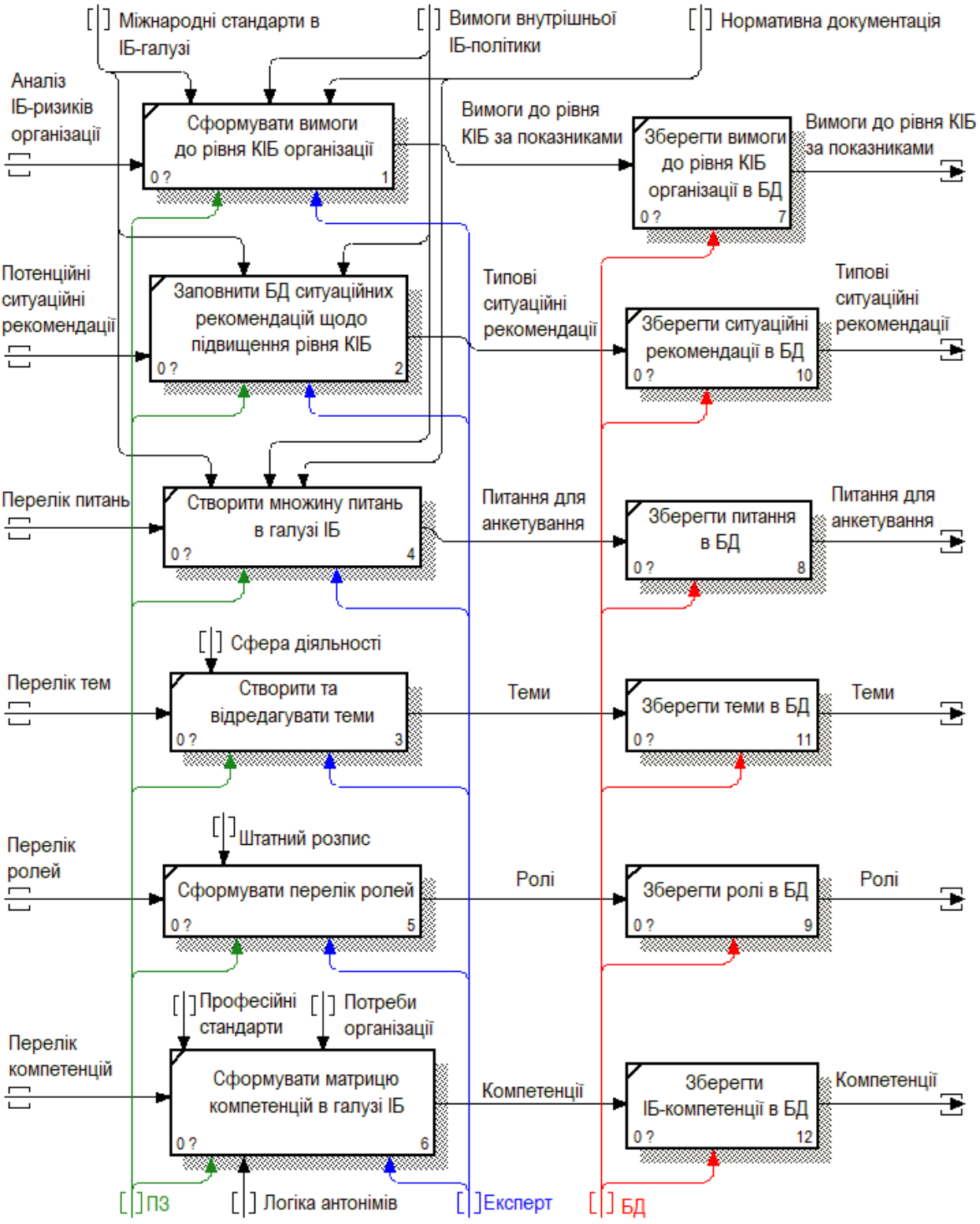

Рисунок 3.3 – Функціональна модель бізнес-процесу третього рівня «Наповнити систему вхідною інформацією» (перший етап)

Кожна задача виконується за підтримки розробленого ПЗ та БД. Невід’ємним учасником є експерт.

Результатом виконання першого етапу є вимоги до рівня КІБ, ситуаційні рекомендації, теми, питання для анкетування, ролі та компетенції.

3.1.3.2 IDEF0 2-го етапу оцінки рівня КІБ організації

Процеси другого етапу представлені на рисунку 3.4. Задача «Згенерувати анкети» поділяється на три підзадачі:

– Розбити масив питань за темами. Масив питань для анкетування поділяється на кластери відповідно до тем за допомогою нечіткої кластеризації. Ступінь належності питання до кожної з тем визначається експертом.

– Призначити вагу впливу кожного питання на результуючу оцінку анкети. Виходячи з набору компетенцій для кожної з ролей, експерт призначає вагові коефіцієнти для кожного питання в межах анкети. Визначення ваг реалізовано на основі методу парних порівнянь.

– Зберегти матрицю ваг у відповідній таблиці БД.

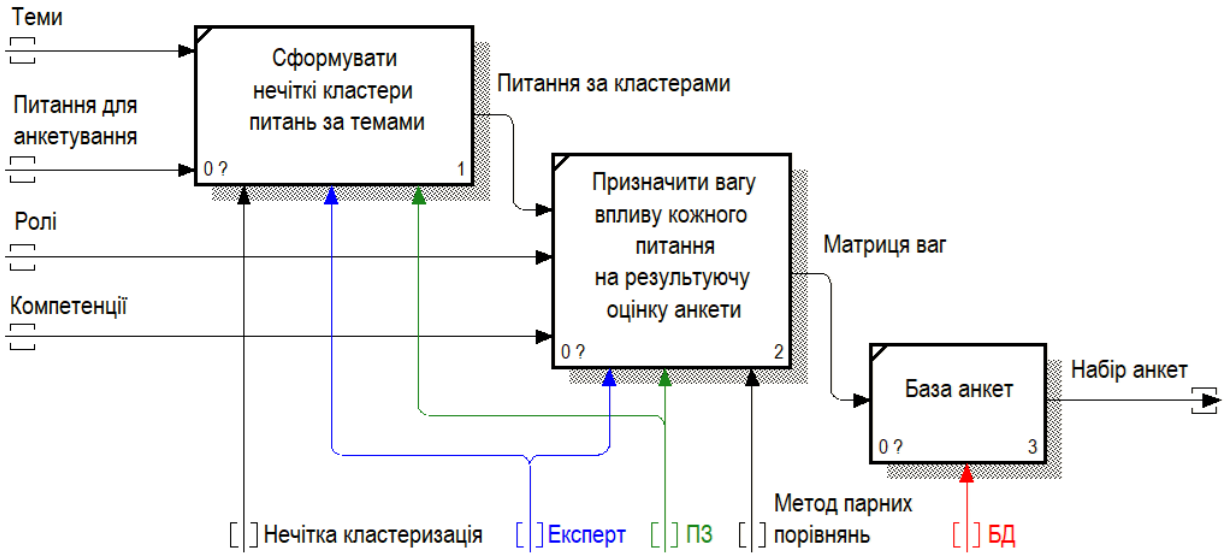

Рисунок 3.4 – Функціональна модель бізнес-процесу третього рівня «Згенерувати анкети» (другий етап)

Результатом опрацювання вхідних даних на другому етапі є створений набір анкет, які відповідають певним ролям та висвічують рівень користувацьких компетенцій за певними темами.

3.1.3.3 IDEF0 3-го етапу оцінки рівня КІБ організації

Етап «Провести анкетування», представлений на рисунку 3.5, передбачає такі завдання:

- Розподілити анкети за посадами. Розподіл анкет, сформованих на попередньому етапі, проводиться експертом згідно ролей, що виконують користувачі (співробітники) в рамках посадових обов'язків. Згенеровані анкети, що представляють собою форму, створену та поширювану за допомогою хмарних сервісів, містять питання та варіанти відповідей.
- Зібрати результати анкетування. Завдання автоматизованого збору результатів також вирішується за рахунок використання хмарних сервісів, оскільки вони дозволяють автоматичне заповнення таблиць такими даними, як дата та час проведення анкетування, контактна електронна адреса, відповіді (обраний пункт або розгорнута відповідь респондента, яка потребує оцінки експерта власноруч). При цьому для анкетування можуть надаватися як типові анкети, так і унікальні, сформовані для кожного користувача окремо.
- Оцінити зібрані результати. Проведення оцінки результатів анкетування здійснюється експертом на основі нечіткої логіки, приймаючи до уваги компетенції, що мають бути наявними у достатній мірі.
- Зберегти результати оцінювання. Оцінки, що є результатом опрацювання відповідей респондентів за допомогою модуля нечіткої оцінки (опис архітектури приведений в п.3.4), зберігаються у БД. Ці записи містять відмітку про час, що дає змогу віднести анкетування до робіт в рамках проведення заходів з оцінки рівня КІБ організації (в якості проекту або етапу процесу), а також спостерігати динаміку персональних КІБ співробітників.

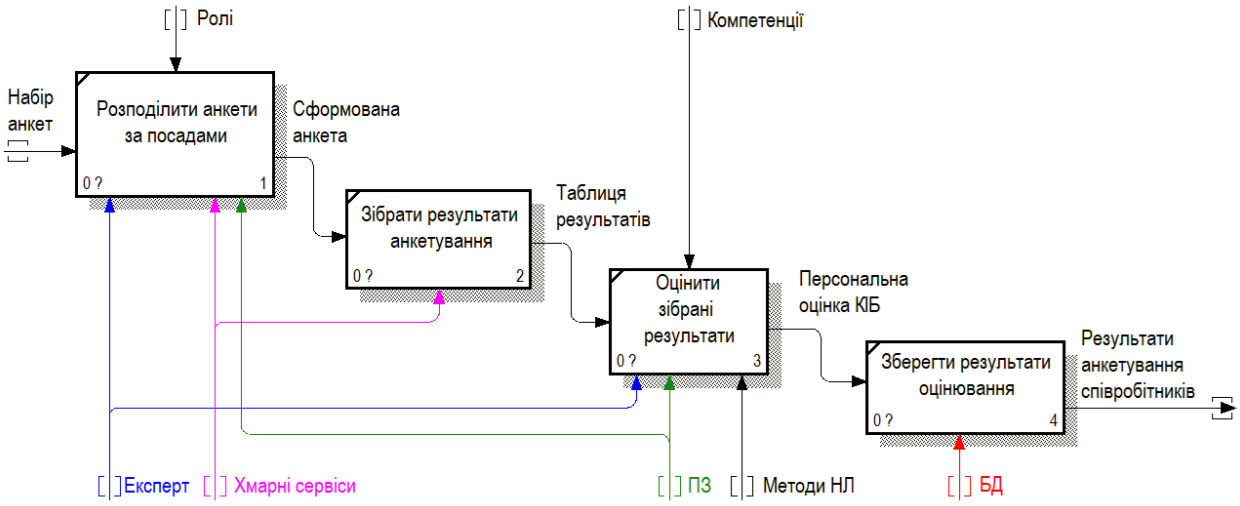

Рисунок 3.5 – Функціональна модель бізнес-процесу третього рівня «Провести анкетування» (третій етап)

3.1.3.4 IDEF0 4-го етапу оцінки рівня КІБ організації

Отримані на попередньому етапі результати оцінки КІБ співробітників є вхідною інформацією для процесу «Оцінити рівень КІБ за підрозділами», що приведений на рисунку 3.6.

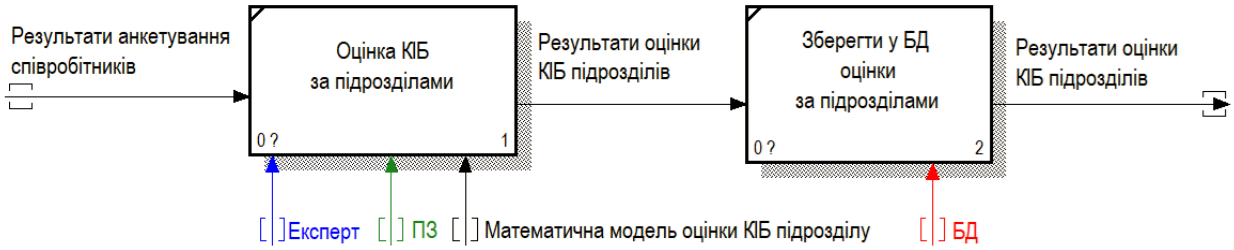

Рисунок 3.6 – Функціональна модель бізнес-процесу третього рівня «Оцінити рівень КІБ за підрозділами» (четвертий етап)

На даному етапі проводиться оцінка рівня КІБ підрозділу, що є результатом визначення персонального рівня КІБ серед працівників, які входять до складу підрозділу. На базі раніше визначеної математичної моделі оцінки КІБ підрозділу експерт отримує результат оцінки КІБ кожного підрозділу. Отримані результати зберігаються у таблиці БД.

3.1.3.5 IDEF0 5-го етапу оцінки рівня КІБ організації

П’ятий етап «Оцінити рівень КІБ організації» (рисунок 3.7), подібно до попереднього, складається з двох підпроцесів:

– Оцінка рівня КІБ організації. Експерт на основі отриманих показників КІБ структурних підрозділів, які є вхідною інформацією блоку, визначає загальну оцінку КІБ організації за допомогою математичної моделі оцінки КІБ організації.
– Зберегти у БД. Запис, що містить результат попереднього процесу, вноситься до БД з відміткою про дату (або період) проведення оцінки.

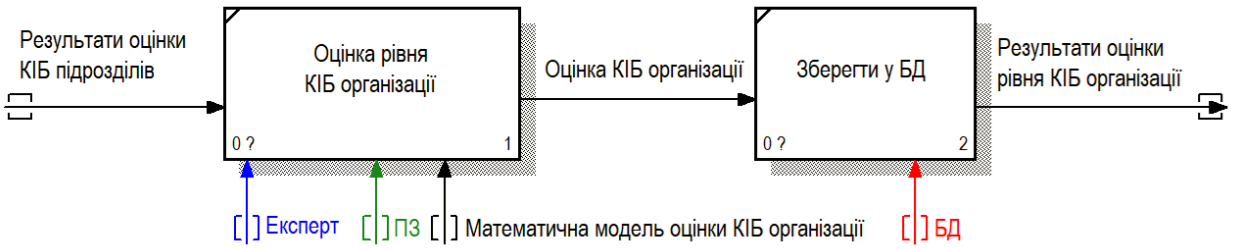

Рисунок 3.7 – Функціональна модель бізнес-процесу третього рівня «Оцінити рівень КІБ організації» (п'ятий етап)

3.1.3.6 IDEF0 6-го етапу оцінки рівня КІБ організації

Завершальний етап оцінки КІБ організації представляє послідовне виконання двох процесів. Декомпозиція бізнес-процесу «Створити звіт та надати рекомендації» представлена на рисунку 3.8. Розглянемо детальніше.

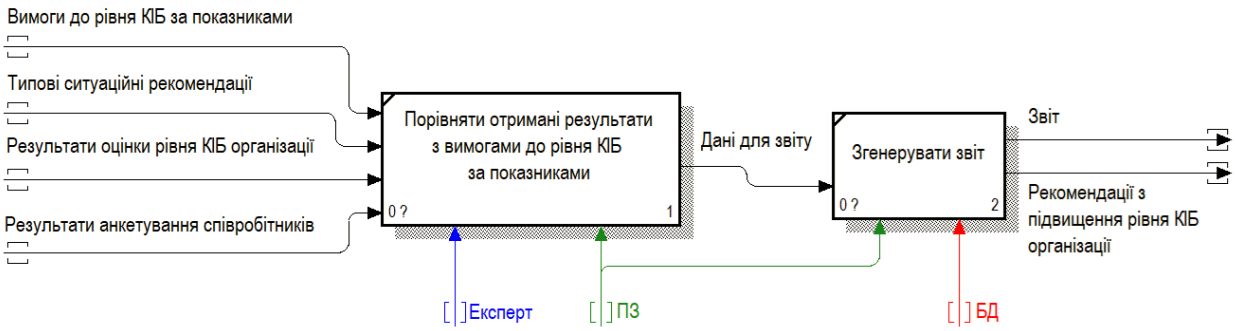

Рисунок 3.8 – Функціональна модель бізнес-процесу третього рівня «Створити звіт та надати рекомендації» (шостий етап)

– Порівняти отримані результати з вимогами до рівня КІБ за показниками. Вхідною інформацією для цього виступають раніше визначені (на першому етапі) вимоги до рівня КІБ за показниками, доступ до наявних у системі типових ситуаційних рекомендацій, а також результати

анкетування співробітників та результати оцінки рівня КІБ організації, що визначені на попередньому етапі. У випадку виявлення результатів, що не задовольняють вимогам, система звертається до бази продукційних правил та визначає відповідну рекомендацію. Набір таких рекомендацій буде включений до звіту.

– Згенерувати звіт. Дані, що отримані після порівняння, складають основу для генерації звіту. З БД вибираються відповідні рекомендації, що стосуються заходів з підвищення рівня КІБ співробітників, а також рекомендації для керівників, які задачі мають бути вирішені на адміністративному рівні. Експерт перевіряє підготовлений звіт.

3.2 Варіанти використання інформаційної системи

Перш ніж розпочати розробку інформаційної системи, слід виділити її основні функціональні можливості.

Основними функціональними вимогами до інформаційної системи є:

– збір, обробка, зберігання інформації, такої як набір питань для формування анкет, результати опитування респондентів, експертна оцінка рівня КІБ (персональна, для структурних одиниць, організації);
– формування і виведення результатів: порівняльний аналіз поточного стану рівня КІБ щодо відповідності вимогам нормативної документації та результатам ризик-аналізу;
– створення, зберігання та удосконалення набору типових рекомендацій щодо підвищення наявного рівня КІБ організації.

На основі бізнес-логіки процесу, що детально представлена в попередньому підрозділі, діаграма відображає основні варіанти використання ІС її акторами (рисунок 3.9). Акторами для системи виступають експерт, керівник або менеджер ІБ-підрозділу, працівник та хмарні сервіси.

Подальша деталізація варіантів взаємодії акторів з системою свідчить про те, що основна взаємодія із системою відбувається з боку Експерта. Актор Експерт взаємодіє з системою напротязі всього процесу оцінювання.

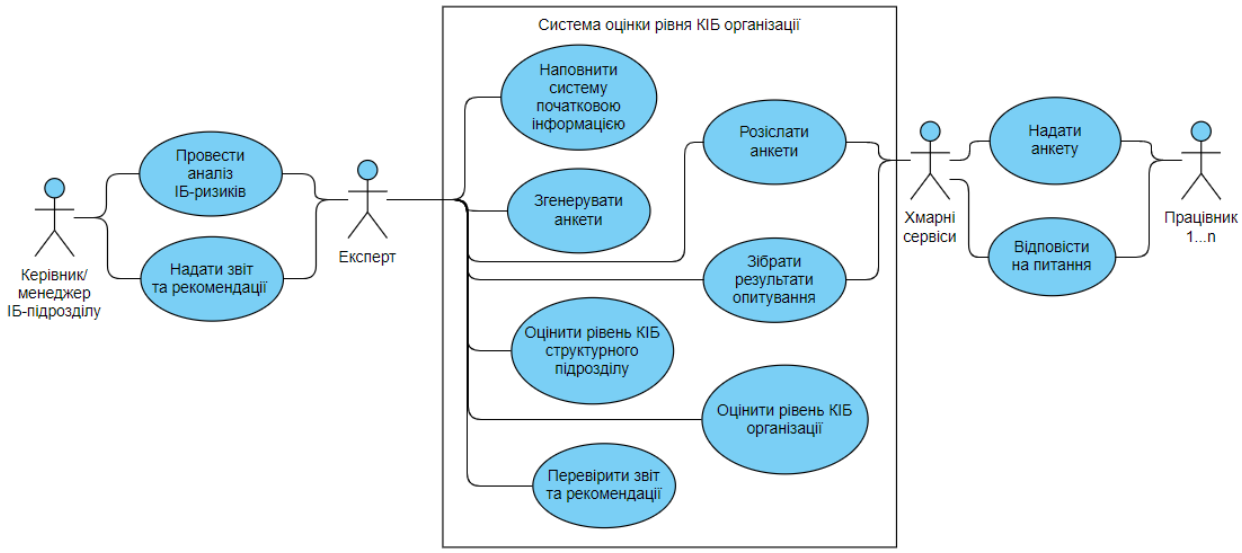

Рисунок 3.9 – Діаграма основних варіантів використання

На етапі наповнення системи початковою інформацією Експерт заповнює таблиці БД системи (формує вимоги до ІБ; наповнює БД типових ситуаційних рекомендацій (заходів), спрямованих на підвищення рівня КІБ співробітників та організації; створює перелік питань для анкетування та розподіляє їх за темами; створює перелік ролей (на базі посад зі штатного розпису); наповнює матриці компетенцій) (рисунок 3.10).

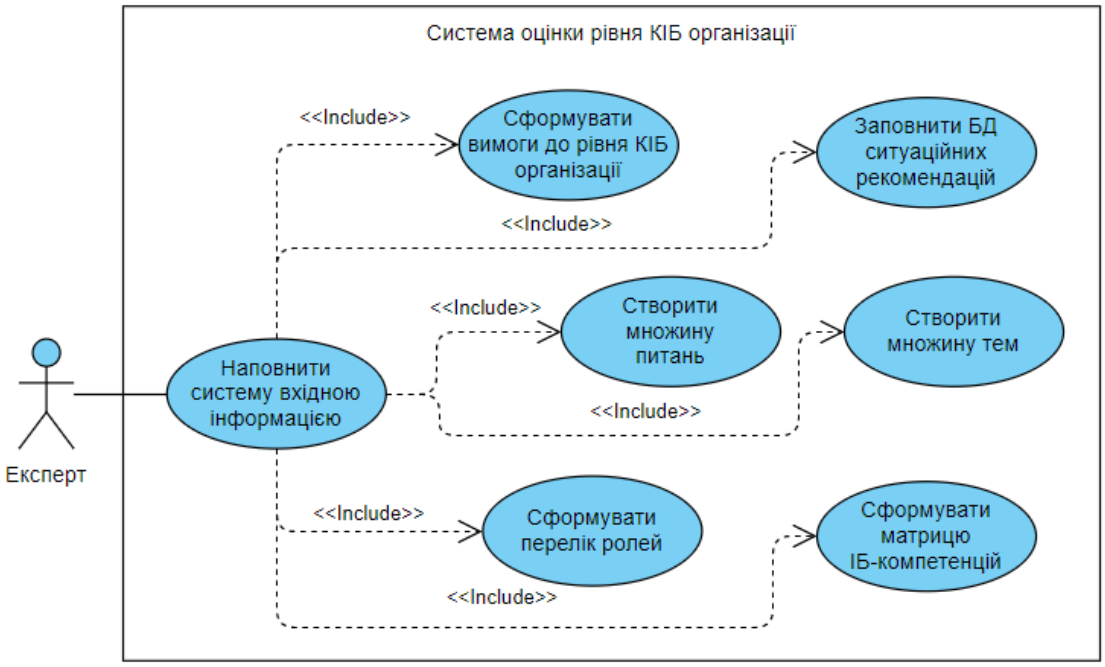

Рисунок 3.10 – Діаграма варіантів використання для актора Експерт при наповненні системи вхідною інформацією

Під час другого етапу Експерт вносить до системи вагові коефіцієнти, що відображають ступінь належності питань до набору тем, вагу кожного питання (вплив на результуючу оцінку анкетування); вплив ролей на загальний рівень КІБ підрозділу; призначає ваги компетенцій в рамках кожної ролі. Експерт формує БП для нечіткої моделі оцінки рівня персональної КІБ працівників, а також БП визначення рекомендацій (рисунок 3.11).

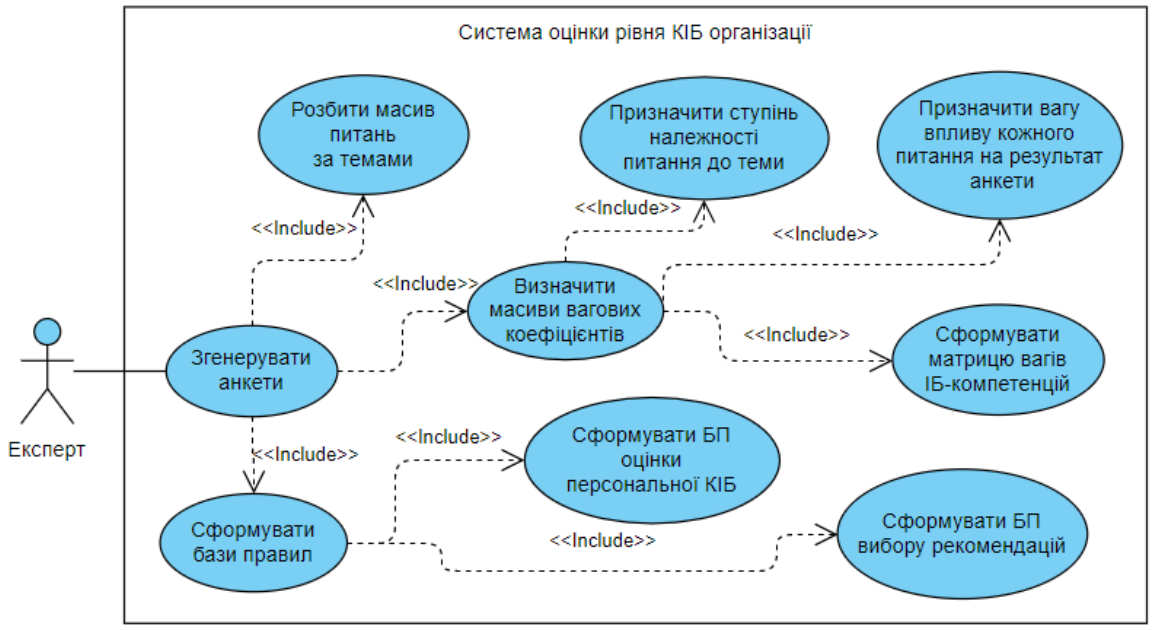

Рисунок 3.11 – Діаграма варіантів використання для актора Експерт при генерації анкет

Для проведення анкетування (рисунок 3.12) Експерт розподіляє анкети за посадами працівників та розсилає за допомогою актора Хмарні сервіси (а саме Google Forms, Microsoft Forms, Visual Paradigm Forms, тощо). Результати анкетування кожного працівника зберігаються у зв’язаній таблиці відповідного сервісу (Google Sheet, Microsoft Excel, Visual Paradigm Form Results, тощо), а згодом копіюються до таблиці БД. Опрацювання результатів оцінки рівня персональної КІБ виконується за допомогою СНВ, зберігається у таблиці БД та формують рівень КІБ відповідного структурного підрозділу, до якого належать працівники.

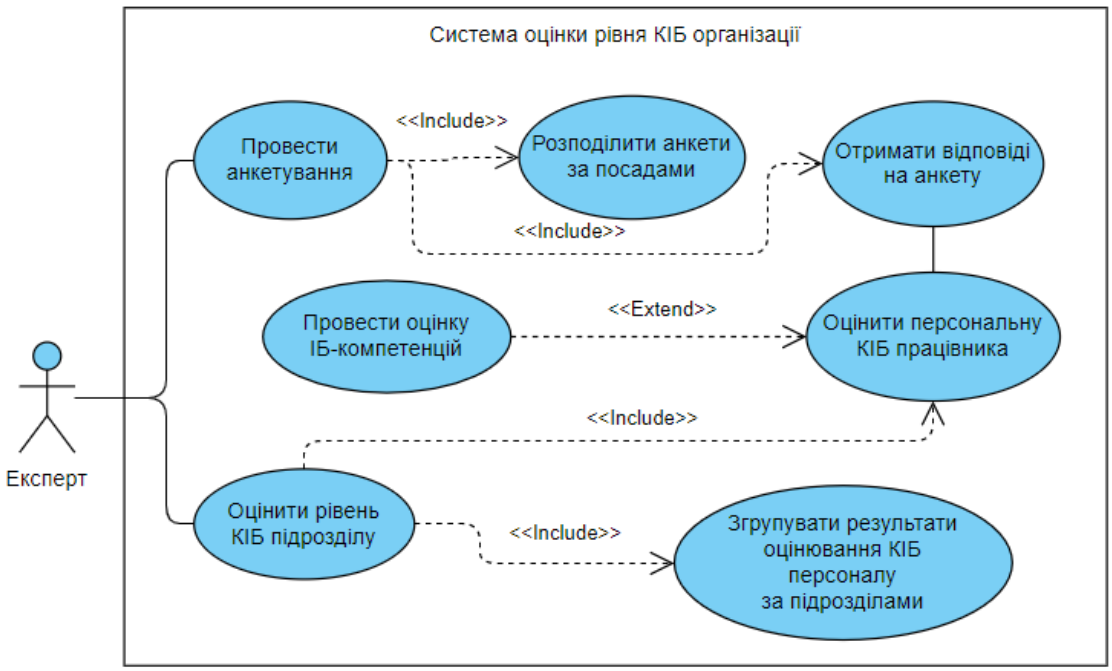

Рисунок 3.12 – Діаграма варіантів використання для Експерта при проведенні анкетування та обрахуванні отриманих результатів

На основі попередніх оцінок рівня КІБ структурних підрозділів проводиться перевірка на відповідність отриманих результатів до висунутих вимог щодо рівня КІБ (рисунок 3.13). Оцінки рівня КІБ за структурними підрозділами є складовими для визначення рівня КІБ організації. Висновок про відповідність встановленим вимогам та набір рекомендацій складають звіт, який генерує система, та надає Експертові на перевірку.

На завершальному етапі актор Експерт перевіряє коректність отриманого звіту та набору рекомендацій для підсилення рівня КІБ організації через впровадження заходів з підвищення обізнаності та практичного досвіду працівників (підвищення персональної КІБ).

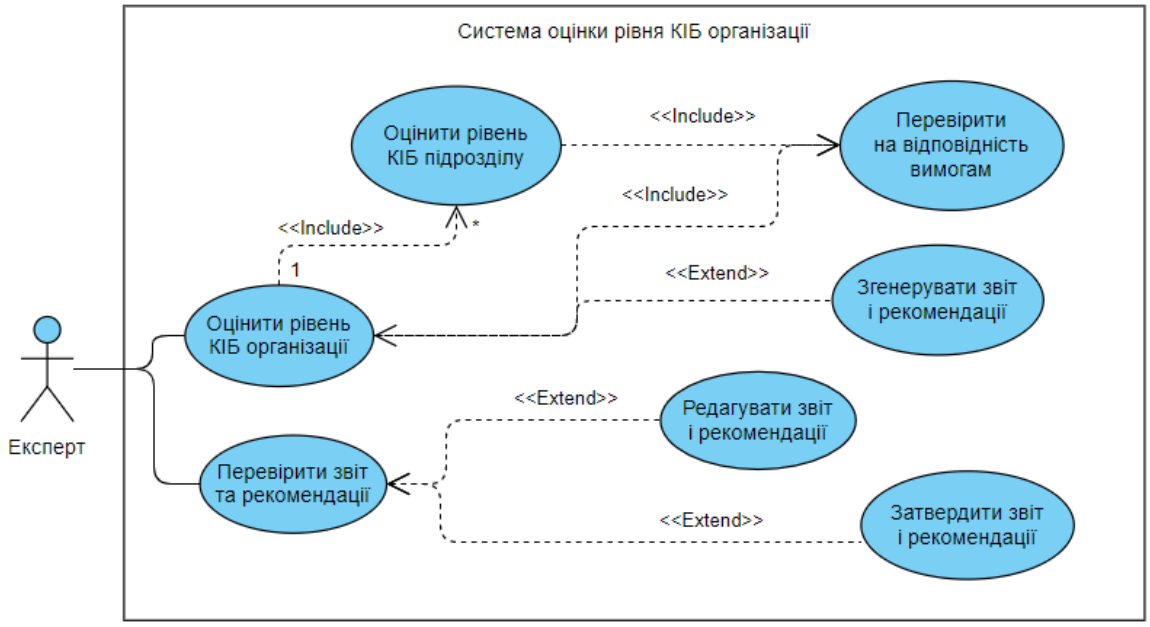

Рисунок 3.13 – Діаграма варіантів використання для Експерта при визначенні рівня КІБ організації та формуванні звіту

Опис інших акторів, їх участі та варіанти їх взаємодії з Експертом можна описати наступними діаграмами.

Керівник або *менеджер ІБ-підрозділу* виступає ініціатором аудиту КІБ для організації, надає експертові інформацію про результати ризик-аудиту ІБ організації, а також надає відомості про загальний стан ІБ організації (рисунок 3.14). За результатами оцінювання КІБ організації він, як її представник, затверджує звіт та рекомендації.

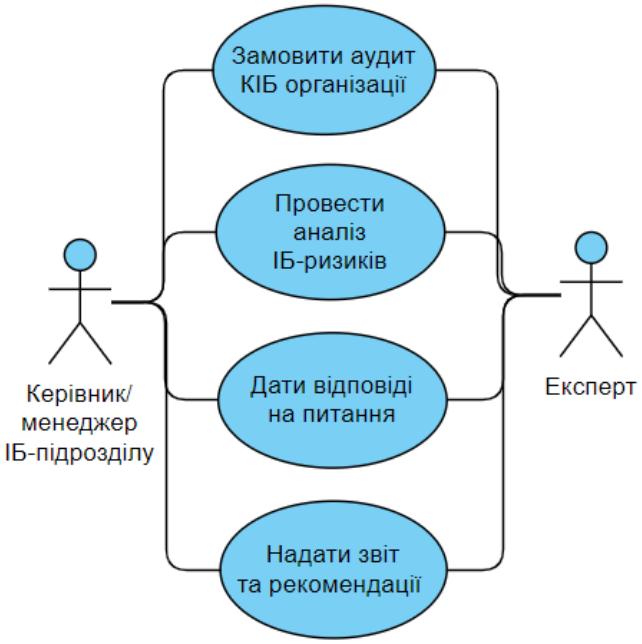

Рисунок 3.14 – Діаграма варіантів взаємодії між Керівником та Експертом

Працівник приймає участь при анкетуванні (рисунок 3.15). За результатами анкетування працівників організації складається оцінка рівня КІБ підрозділів, що в подальшому формує оцінку рівня КІБ організації.

Хмарні сервіси. Анкетування проводиться в режимі онлайн за допомогою анкет-форм, що створені та поширюються за підтримки хмарних сервісів (Google Forms, Microsoft Forms, Visual Paradigm Forms, тощо).

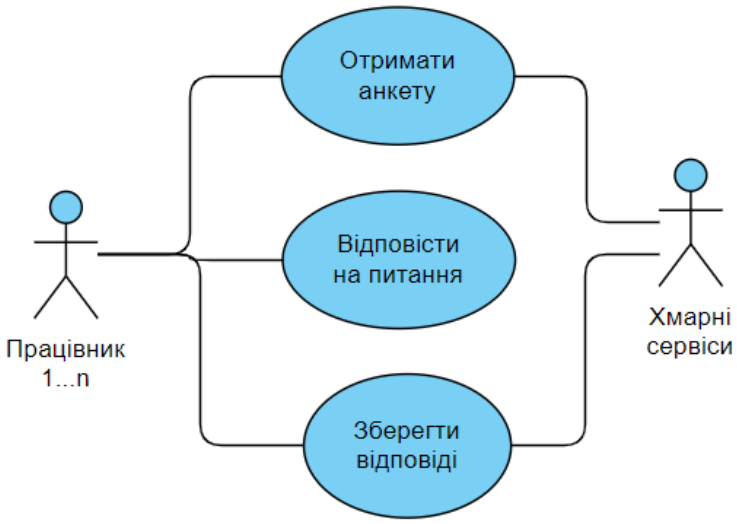

Рисунок 3.15 – Діаграма варіантів взаємодії Працівника з Хмарними сервісами під час анкетування

Працівник не має безпосередньої взаємодії із системою, оскільки анкетування проводиться через хмарні сервіси. Результати анкетування накопичуються спочатку у відповідних таблицях, що пов’язані із формами-анкетами, а згодом завантажуються у таблицю БД системи.

3.3 Взаємодія модулів інформаційної системи

В рамках проведення оцінки рівня КІБ організації актори взаємодіють із модулями системи у визначеному порядку. Діаграма послідовності дій представлена на рисунку 3.16.

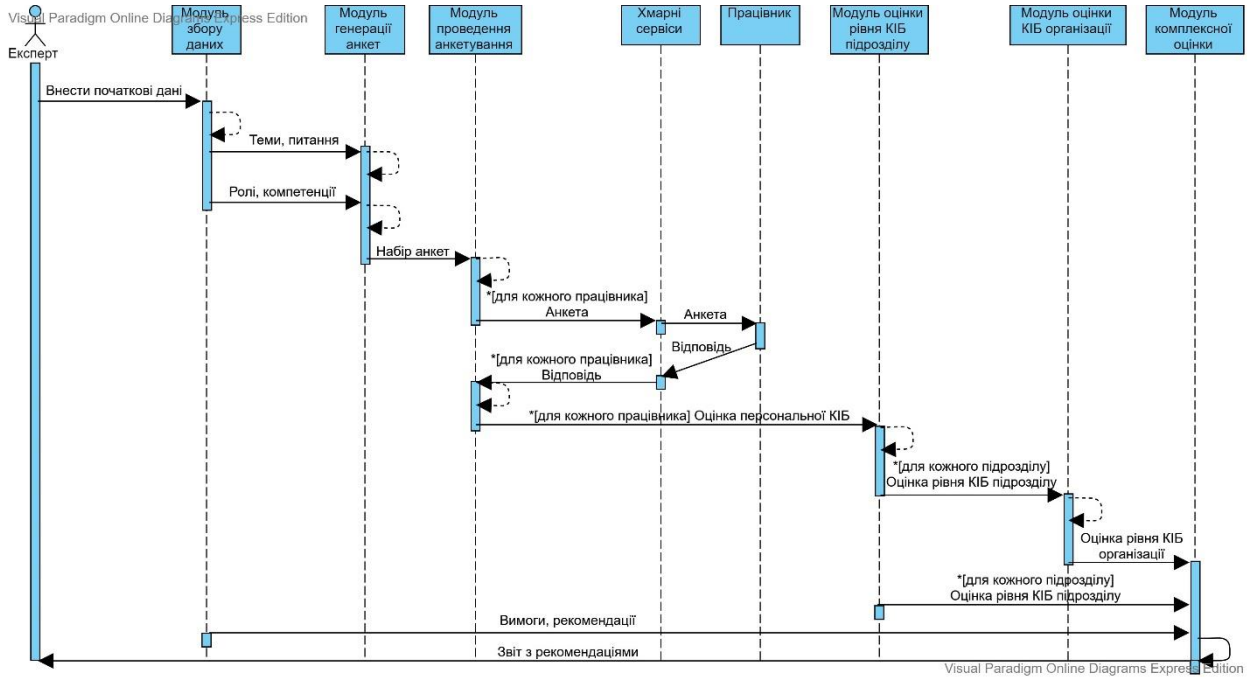

Рисунок 3.16 – Діаграма послідовності дій при взаємодії з модулями системи

Наповнення системи початковою інформацією (питання, теми, ролі, посади, компетенції, вимоги та ситуаційні рекомендації) відбувається через взаємодію експерта із Модулем збору даних. Інформація, що підготовлена експертом, зберігається у відповідних таблицях БД.

На етапі створення масивів питань експерт розподіляє питання за тематиками (використовуючи нечітку кластеризацію).

Одна із діаграм класів наведена на рисунку 3.17.

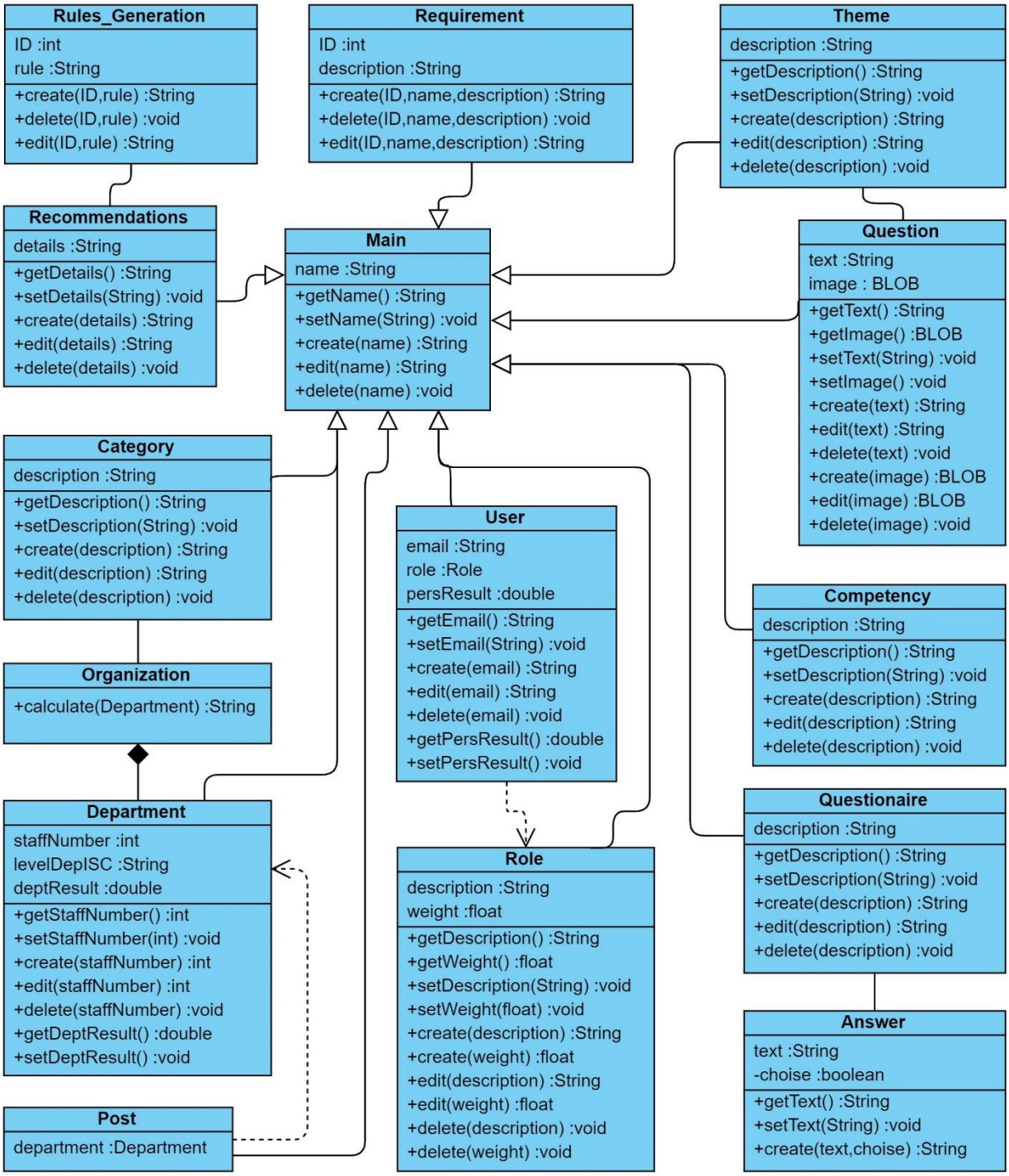

Рисунок 3.17 – Діаграма класів інформаційної системи

3.4 Архітектура інформаційної комп’ютерної системи

Для реалізації поставлених задач запропоновано архітектуру інформаційної комп’ютерної системи визначення рівня КІБ організації [114, 120], зображену на рисунку 3.18.

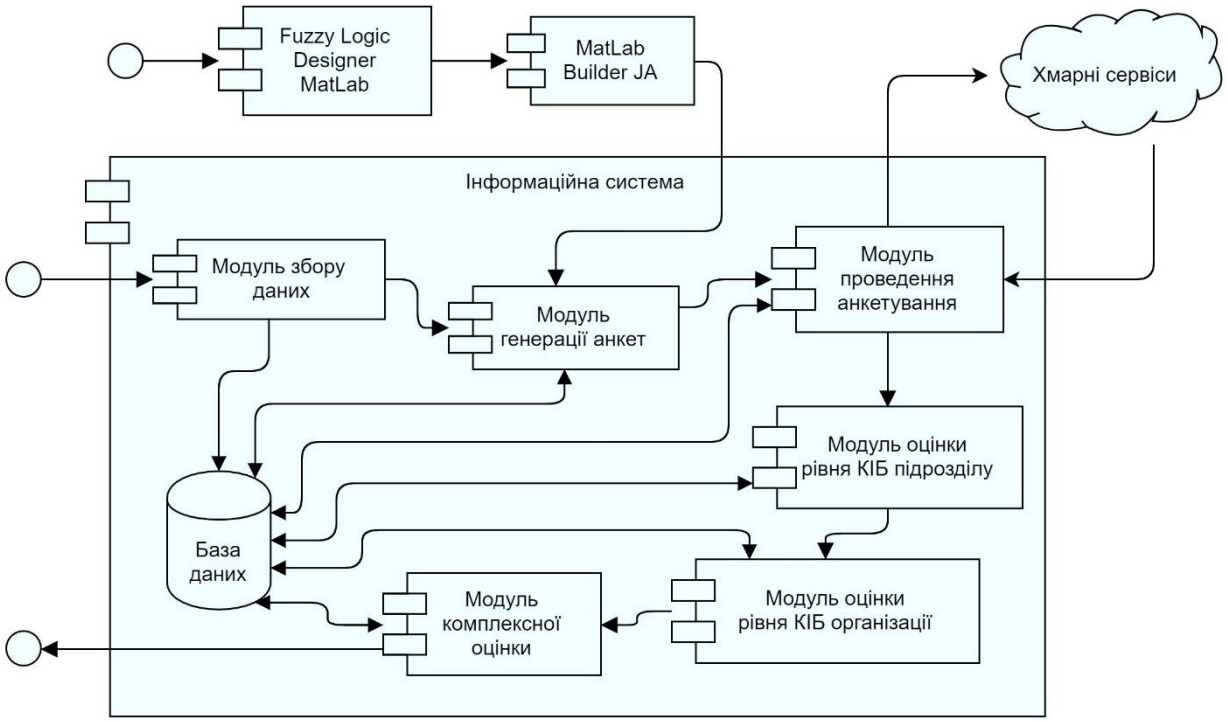

Рисунок 3.18 – Архітектура інформаційної комп’ютерної системи для визначення рівня КІБ організації

Система складається з 6 основних модулів:

- модуль збору даних, призначений для того щоб експерт (або група експертів) з інформаційної безпеки мав змогу наповнювати базу даних усією необхідною інформацією для подальшої генерації анкет та проведення оцінки;
- модуль генерації анкет, розподіляє питання для анкет за тематиками, після чого за допомогою експертної оцінки методом парних порівнянь визначаються ваги питань з врахуванням набору компетенцій та ролей працівників, які проходять анкетування або тестування;
- модуль проведення анкетування надає доступ співробітникам організації до анкети та зберігає у базі результати анкетування або виконання тестів;
- модуль оцінки рівня КІБ підрозділу за результатами заповнених анкет або виконаних тестів формує загальну оцінку рівня КІБ за підрозділами організації;

– модуль оцінки рівня КІБ організації формує загальний рівень КІБ всієї організації, виходячи з оцінки всіх підрозділів;
– модуль комплексної оцінки генерує звіт за результатами проведеного тестування працівників та виходячи з визначеного рівня культури інформаційної безпеки організації надає рекомендації, які спрямовані на його підвищення.

3.5 База даних

Для інформаційної системи оцінювання рівня КІБ організації [114] невід'ємною частиною є БД, логічна модель якої представлена на рисунку 3.19.

Основні сутності моделі БД:

- «Тема»;
- «Питання»;
- «Відповідь»;
- «Результат відповіді»;
- «Категорія критичності»;
- «Вимога»;
- «Рекомендація»;
- «Компетенція»;
- «Роль»;
- «Користувач»;
- «Посада»;
- «Підрозділ»;
- «Анкета»;
- «Анкетування»;
- «Оцінювання користувача»;
- «Оцінювання підрозділу»;
- «Оцінювання організації».

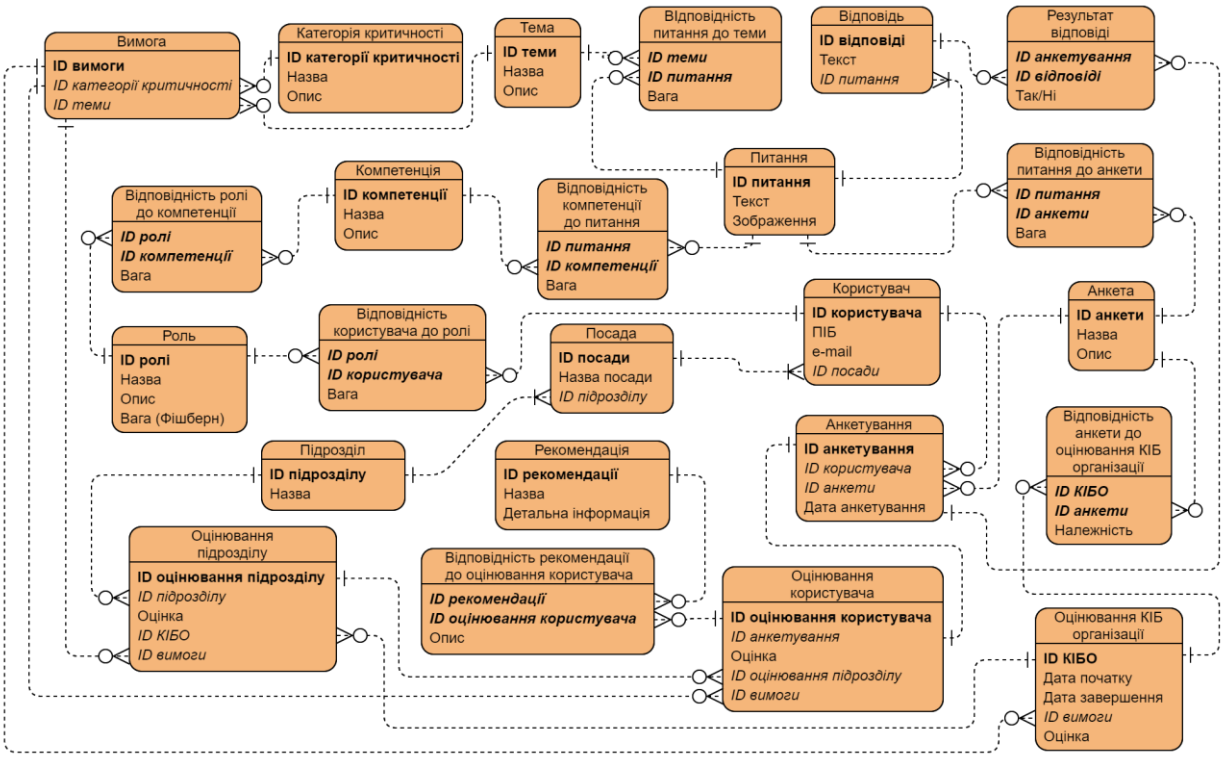

Рисунок 3.19 – Логічна модель БД

Зупинимося на найбільш істотних взаємозв’язках між сутностями, які використані у БД.

В межах анкети питання можуть стосуватися як окремої теми, так і суміжних. Ступінь належності питання до теми встановлюється експертом та міститься в таблиці «Відповідність питання до теми». Вплив питання на загальну оцінку анкети також визначається експертом та вноситься до таблиці «Відповідність питання до анкети».

Кожне «Питання» пов’язане з декількома записами таблиці «Відповідь». Вибір відповіді користувачем на певне питання визначається встановленням відмітки про розміщення «прапорця» (тип Boolean, варіант true/false) – «Результат відповіді».

Таблиця «Анкетування» містить дані про анкету, що була сформована, та відповідного користувача, якому вона була надана для заповнення. «Користувач» пов’язаний з відповідною «Посадою», що він займає в межах «Підрозділу».

Таблиця «**Оцінювання користувача**» пов’язує відповідну анкету (поле «Анкетування»), «Користувача», оцінку, що отримана в результаті опрацювання даних модулем нечіткої оцінки персональної КІБ, належність користувача до певного підрозділу, а також ідентифікатор вимоги, яка має бути виконана за рахунок наявності у «Користувача» певної «Компетенції».

«**Оцінювання підрозділу**» отримує результат після опрацювання модулем оцінки КІБ підрозділу, що зберігається відповідним записом «Оцінка», а також містить інформацію про власне «Підрозділ», належність до певного заходу «ID КІБО» та «Вимоги», з якими пов’язана діяльність підрозділу.

Таблиця «**Оцінювання КІБ організації**» має поля початку та завершення оцінювання. Це дозволяє ідентифікувати набір отриманих результатів анкетування як ті, що проведені в рамках одного заходу.

«**Відповідність анкети до оцінювання рівня КІБ організації**» визначається булевою змінною, її значенням «Так/Ні» (true/false), що вказує на те, чи була дана анкета задіяна в рамках проведення оцінки рівня КІБ організації.

Таблиця **«Категорія критичності»** слугує основою для формування вимог до ІБ, виходячи з належності організації до категорії критичності об’єкта інфраструктури. Також при наповненні таблиці «**Вимога**» враховується результат ІБ-ризик-аналізу організації.

Висновки до розділу 3

Запропонована концепція інформаційної системи, яка дозволяє визначити поточний рівень КІБ організації, виходячи з результатів оцінки обізнаності співробітників в галузі інформаційної безпеки. Рекомендації щодо заходів з підвищення рівня КІБ формуються з врахуванням ризик-аналізу в галузі ІБ та вимог згідно класу критичності організації або підприємства. Для реалізації інформаційної системи запропоновано архітектуру, що представлена 6 модулями, які забезпечують послідовне виконання

технологічних етапів оцінювання КІБ. Основними перевагами цієї системи можна зазначити наступні:

1) Використання нечітких множин звільняє від необхідності проводити інструментальні вимірювання показників, проте дозволяє отримувати кількісні оцінки шляхом дефазифікації якісних показників.
2) Система передбачає можливість створення унікальних моделей (таких як модель ІБ-компетенцій користувачів, структурна модель організації, ролі в рамках посадових обов'язків, та ін.) залежно від класу критичності, до якого належить організація.
3) Використання бази правил забезпечує спрощене створення та редагування СНВ, що, знов ж таки, реалізує можливість адаптації інформаційної системи до оцінювання об'єктів будь-якого класу критичності.
4) Запропонована система враховує відповідність наявних ІБ-компетенцій працівників до вимог, аналіз системи заходів з розвитку КІБ організації та її підтримки на належному рівні, ступінь розвитку співпраці з державними та міжнародними спеціалізованими спільнотами, тощо. За результатами оцінювання система формує набір рекомендацій а рівні структурної одиниці та користувача, а також загальну оцінку рівня КІБ організації.

Результати досліджень, приведених в розділі, опубліковані в роботах [114, 120].

РОЗДІЛ 4
ЗАСТОСУВАННЯ ЕЛЕМЕНТІВ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ

4.1 Проведення експерименту з визначення персонального рівня КІБ користувачів

Висвітленню експерименту присвячені роботи [72, 91]. Оскільки фізичне вимірювання показників КІБ неможливо, запропоновано вдатися до опитування респондентів з подальшою обробкою результатів. Для визначення рівня особистої КІБ розроблена анкета, яка містить ясні та стислі відповіді. Для збереження зацікавленості учасників опитування займає не більше 5-7 хвилин у респондентів. Збільшення кількості запитань або пропозиція сформувати детальну відповідь призведе до втрати інтересу серед учасників і негативно вплине на результати заключних питань. Опитування проводилося на добровільних засадах та із збереженням анонімності (без збору електронних адрес). Для складання анкети були використані Рекомендації [121].

Цільова аудиторія представлена студентами спеціальності 121-«Інженерія програмного забезпечення» та учасниками проектів, які реалізуються кафедрою інформаційних технологій та програмної інженерії Чернігівського національного технологічного університету.

Метою опитування є отримання даних з первинних джерел про використання інструментів та методів кіберзахисту кінцевими користувачами в їх повсякденній діяльності (навчання, робота, проектна діяльність та відпочинок). У той же час опитування учасників виправдовується тим, що вони є активними користувачами внутрішнього інформаційного простору під час діяльності, а сформовані основи персональної кібербезпеки, як фрагмент особистої КІБ, впливають на навчальну, професійну та проектну діяльність.

Анкета містить 9 питань, які висвітлюють основні положення основ персонального кіберзахисту. Ймовірність помилки при заповненні анкети зводиться до мінімуму за рахунок надання різноманітних та найбільш чітко

складених варіантів відповідей. Питання логічно згруповані в 3 блоки та зосереджені на забезпеченні захисту облікових записів, особистих гаджетів та операційних систем (ОС).

За результатами опитування 39,5% респондентів надають перевагу користуванню ОС з правами адміністратора (рисунок 4.1); 52,6% використовують один спільний обліковий запис в робочих та особистих цілях (рисунок 4.2). Високу активність у соціальних мережах ведуть 18,4% учасників та регулярно оновлюють інформацію та фотографії (рисунок 4.3). Така ж доля респондентів використовує особисті сторінки в соціальних мережах для зберігання цікавої для них інформації. 39,5% респондентів є рідкими відвідувачами власних сторінок, а 21,1% втратили інтерес до соціальних мереж.

Рисунок 4.1 – Результати опитування щодо типів облікових записів в ОС

Рисунок 4.2 – Результати опитування щодо використання спільних акаунтів та гаджетів

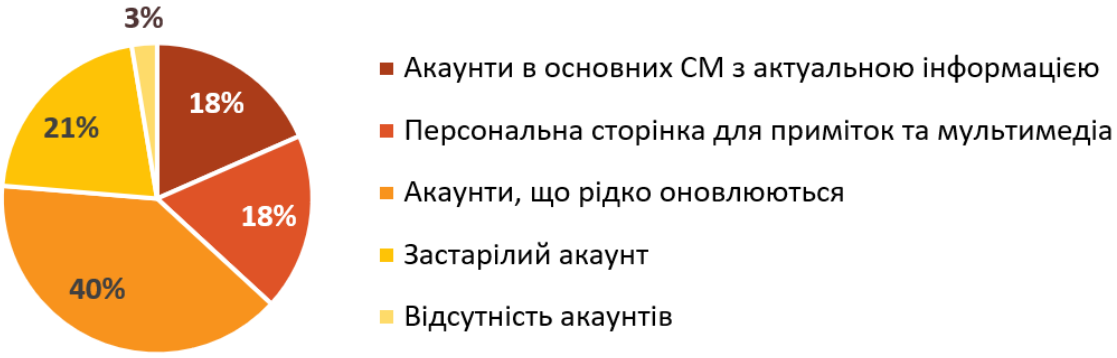

Рисунок 4.3 – Результати опитування щодо розподілу облікових записів

47,4% респондентів стежать за актуальністю програмного забезпечення за допомогою автоматичних оновлень ОС та програмного забезпечення (рисунок 4.4). 44,7% віддають перевагу підходу вибіркового оновлення. У той же час 44,7% респондентів не встановили жодного антивірусного програмного забезпечення (рисунок 4.5), і лише 21,1% учасників проводять регулярні антивірусні перевірки власної системи (рисунок 4.6).

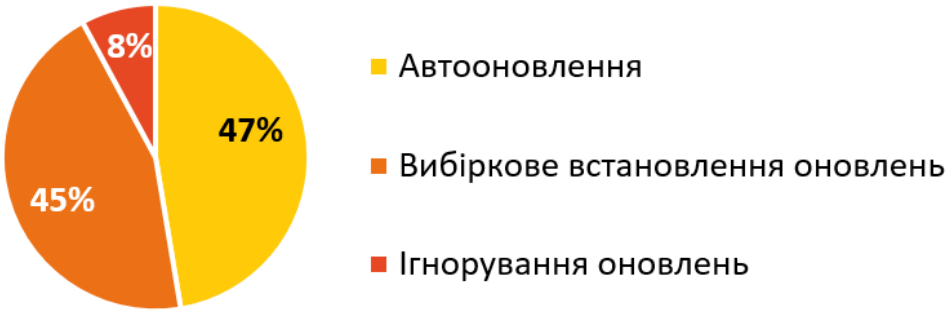

Рисунок 4.4 – Результати опитування: оновлення ОС та ПЗ

Рисунок 4.5 – Результати опитування: наявність антивірусних засобів

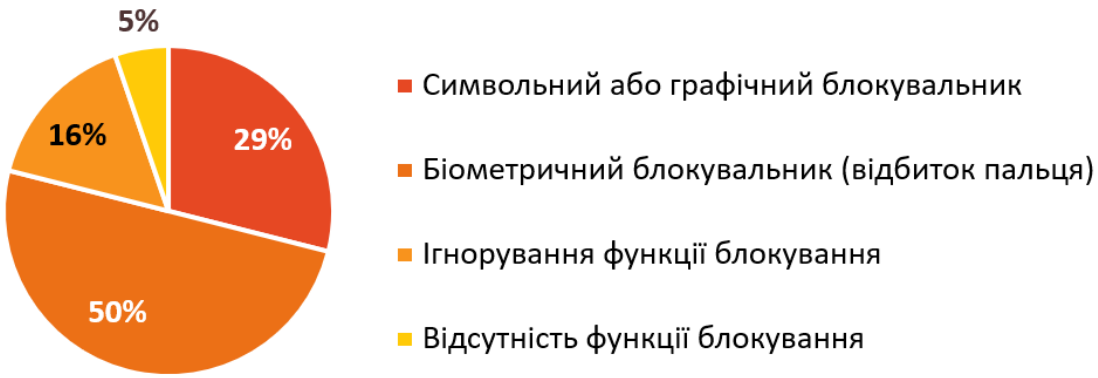

Рисунок 4.6 – Результати опитування: блокування доступу до гаджетів

Половина (50%) респондентів вважають за краще захищати свої гаджети біометричним ключем, 28,9% респондентів використовують символьні або графічні блокувальники (рисунок 4.7).

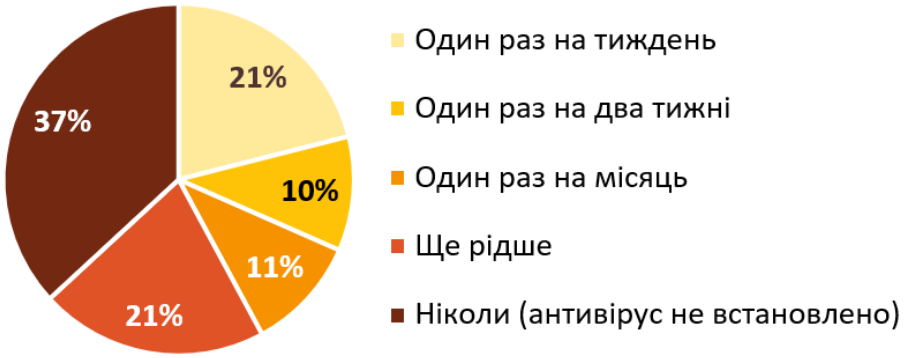

Рисунок 4.7 – Результати опитування: використання АВ-засобів

Стосовно політики паролів (рисунок 4.8), 15,8% респондентів використовують «надійні» паролі для кожного облікового запису, а потім зберігають їх за допомогою менеджера паролів; 21,1% зберігають унікальні паролі на фізичних носіях (ноутбуках, окремих файлах). Більшість опитаних (44,7%) вважають за краще використовувати декілька пам'ятних паролів для більшості випадків реєстрації. Інші респонденти використовують однаковий пароль для всіх облікових записів або використовують автоматичне збереження пароля у веб-браузері.

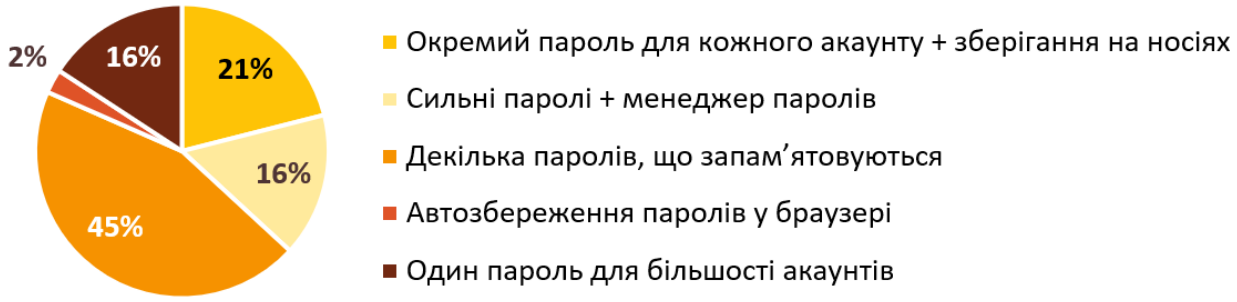

Рисунок 4.8 – Результати опитування: парольна політика

У той же час 65,8% респондентів активно використовують Інтернет-банкінг, що зумовлює низку вимог до культури інформаційної безпеки кінцевого користувача (рисунок 4.9).

Рисунок 4.9 – Результати опитування: використання сервісів онлайн-банкінгу

Варіанти відповідей оцінені за допомогою лінгвістичних оцінок. Для стислості, оцінки описані п’ятьма термами: L – критично слабкий захист; ML – неприйнятний захист; M – прийнятний захист; MH – достатній захист; H – високий захист. Загальні результати опитування представлені на рисунку 4.10.

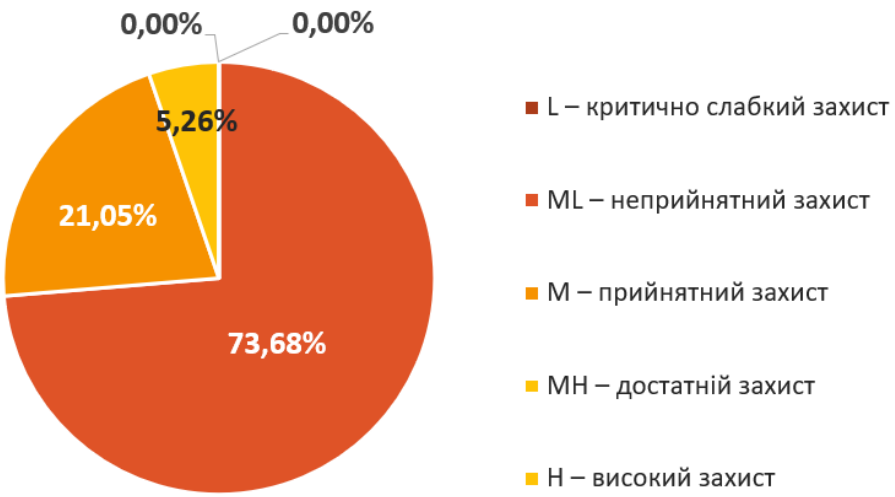

Рисунок 4.10 – Результати опитування

Результати показують, що під час виконання робочих та щоденних рутин 52,6% користувачів користуються одним обліковим записом. 39,5% респондентів працюють з правами адміністратора ОС, які надають можливість прихованого доступу від імені адміністратора. 18,4% учасників активні у соціальних мережах: вони регулярно оновлюють власні особисті сторінки, 18,4% користуються особистими сторінками як сховищем корисної інформації. 44,7% користувачів не встановлюють і не активують антивірусне програмне забезпечення на власних ноутбуках. В інших випадках сканування системи проводиться рідше, ніж раз на тиждень. Політика щодо паролів у 44,7% випадків може бути описана як кілька пам'ятних паролів для більшості випадків реєстрації. У той же час 65,8% респондентів активно використовують Інтернет-банкінг, що зумовлює низку вимог до культури інформаційної безпеки кінцевого користувача.

Проведені за допомогою анкетування дослідження персональної культури інформаційної безпеки учасників науково-дослідного проекту на базі ЧНТУ та оброблені методами нечіткої логіки показали загальний рівень «неприйнятний захист». Це свідчить про наявність високого ризику реалізації загроз КМ через персонал навіть при використанні самих сучасних технологій захисту корпоративних мереж.

Після проведеної Другої весняної кібершколи повторне опитування показало підвищення показників персональної інформаційної культури.

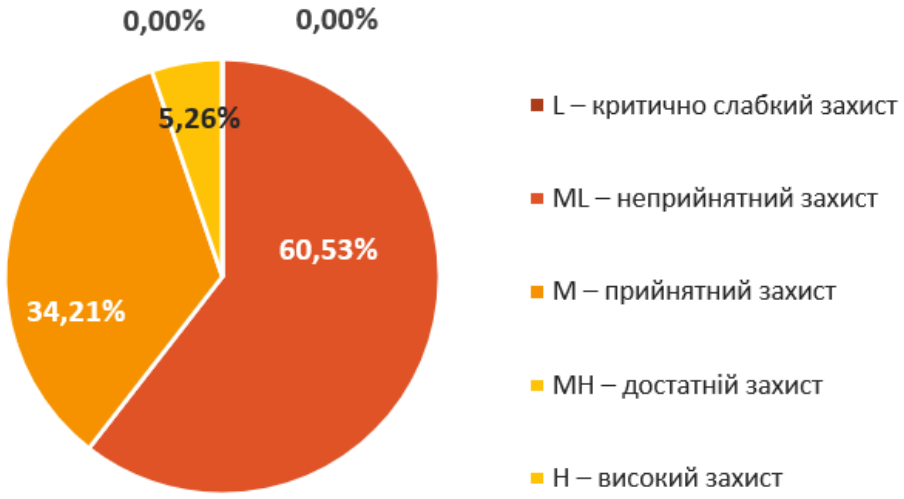

Рисунок 4.11 – Результати анкетування після навчання

Найбільш сильно на результати повторного оцінювання вплинули зміни у таких напрямках, як перехід до розподілу акаунтів за призначенням, зниження активності у соціальних мережах, зростання частоти оновлення ПЗ та посилення парольної політики.

4.2 Компетентність співробітників як інтегральний показник культури інформаційної безпеки персоналу

В рамках науково-дослідної роботи «Розвиток базового моделюючого комплексу мережі ситуаційних центрів державних органів сектору безпеки і оборони України в інтересах захисту критичної інфраструктури держави та кібербезпеки» організаційна культура Центру невід'ємно пов'язана з КІБ. Так, вимоги, що висуваються до персоналу Центрів, зосереджені не лише на професійній діяльності, але і звертають увагу на персональну КІБ кожного співробітника або претендента на посаду. Структура ЦКБ ПЕК та вимоги до персоналу розроблені з врахуванням рекомендацій Карсона Циммермана [122].

4.2.1 Цільова організаційна структура ЦКБ

Типова організаційна структура кіберцентру передбачає наявність основних структурних підрозділів та наведена на рисунку 4.11.

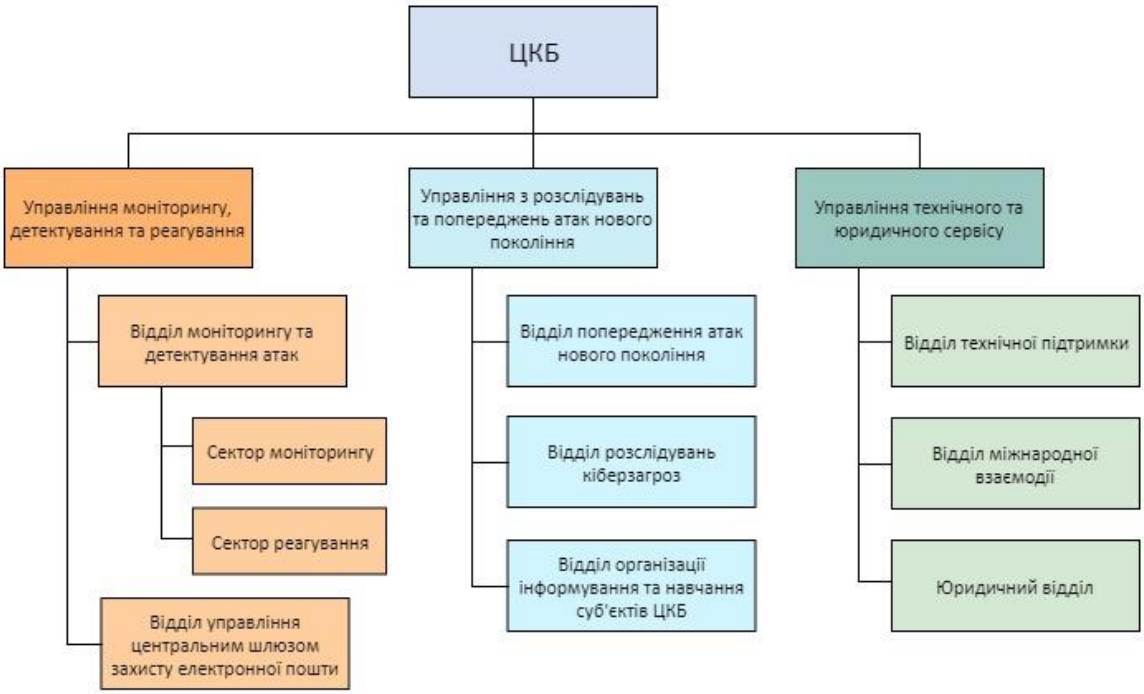

Рисунок 4.12 – Організаційна структура ЦКБ ПЕК

4.2.2 Розподіл функцій між структурними підрозділами ЦКБ

Типові функції структурних підрозділів:

1 Управління моніторингу, детектування та реагування:

1.1 Відділ моніторингу та детектування мережевих атак:

1.1.1 Сектор моніторингу:

- забезпечення телеметрії з приладів, що розташовані в державних підприємствах та об’єктах критичної інфраструктури;
- здійснення відбору даних, що мають підозрілі характеристики;
- взаємодія з Сектором реагування;
- забезпечення функції Гарячої лінії (Call Center) для зв’язків з суб’єктами CyberNet;

- захист веб-доступу та веб-трафіку.

1.1.2 Сектор реагування на мережеві атаки:

- виявлення мережевої розвідки і зондування;
- виявлення та блокування відомих загроз та атак у відповідності до правил і сигнатур;
- виявлення та блокування центрів керування бот-нетами (C&C);
- відстеження та попередження спроб поширення шкідливого ПЗ (malware);
- захист від DoS/DDoS атак.

1.2 Відділ управління центральним шлюзом захисту електронної пошти:

- захист електронної пошти суб'єктів CyberNet за допомоги централізованих сервісів підтримки електронної пошти та Інтернет-комунікацій;
- фільтрування шкідливого коду;
- виявлення спаму та фішингових атак у поштових повідомленнях;
- взаємодія з Відділом технічної підтримки.

2 Управління з розслідувань та попереджень атак нового покоління:

2.1 Відділ попередження атак нового покоління:

- збір та кореляція подій безпеки, даних про мережеву телеметрію;
- раннє виявлення індикаторів компрометації та слідів цільових атак;
- розширений аналіз нових типів шкідливого ПЗ;
- моніторинг протидії загрозам на об'єктах шляхом проведення на об'єктах критичної інфраструктури відповідних тестів, досліджень та розробок;
- відстеження нових тенденцій методів та засобів захисту;
- розробка нових методів та підходів захисту ІБ суб'єктів CyberNet;
- оцінка та прогнозування наявних та можливих загроз в галузі;
- виявлення та попередження нових типів атак за допомогою аналізу мережевої поведінки та аномалій;

- виявлення невідомих загроз «0-дня»;
- оцінка загроз;
- розробка заходів, спрямованих на попередження, реагування та усунення наслідків інцидентів.

2.2 Відділ розслідувань кіберзагроз:

- фіксація виявлених інцидентів;
- збір, накопичення та зберігання даних щодо інцидентів.
- взаємодія із СБУ, ДССЗЗІ та міжнародними організаціями в рамках проведення розслідувань інцидентів;
- проведення розслідувань інцидентів згідно нормативно-правової бази України.

2.3 Відділ організації інформування та навчання суб’єктів ЦКБ:

- надання вичерпної інформації стосовно нормативної та законодавчої бази кібербезпеки;
- інформація для впровадження СЗІБ, СМІБ;
- розробка політик кібербезпеки;
- встановлення обов’язкових вимог інформаційної безпеки об’єктів критичної інформаційної інфраструктури ПЕК, у тому числі під час їх створення, введення в експлуатацію, експлуатації та модернізації з урахуванням міжнародних стандартів та специфіки галузі, до якої належать відповідні об’єкти критичної інформаційної інфраструктури. Контроль за їх виконанням.
- розробка заходів щодо посилення загальної ситуаційної обізнаності щодо інцидентів та вразливостей у середовищі галузевих установ та на об’єктах їх критичної інфраструктури;
- розробка заходів з обміну інформацією та координація дій для зменшення поточних вразливостей, попередження нових та, у разі виникнення загроз, ефективної їх локалізації; критичної інфраструктури, забезпечення інформаційної безпеки та кібербезпеки;

– планування, організація та проведення кібернавчань.

3 Управління технічного та юридичного сервісу

3.1 Відділ технічної підтримки:

– експлуатація та технічне обслуговування інфраструктури SOC;
– встановлення, налаштування та обслуговування сенсорів;
– організація та підтримка відновлення працездатності систем об’єктів критичної інфраструктури;
– автоматизація та програмна підтримка методів моніторингу, виявлення, реагування та відновлення працездатності систем об’єктів критичної інфраструктури;
– проведення досліджень, проектування, розробка та розгортання нових інструментів забезпечення ефективної роботи CyberCenter;
– написання нових сигнатур виявлених шкідливих кодів;
– збір та зберігання матеріалів та результатів аудитів.

3.2 Відділ міжнародної взаємодії:

– налагодження комунікацій з побідними центрами;
– обмін актуальною інформацією;
– взаємодія під час спільної протидії загрозам, при виявленні міжнародних інцидентів, кібертерористичних кампаній тощо.

3.3 Юридичний відділ:

– виконання типових функцій Юридичного відділу організацій:
    а) Забезпечує правильне застосування в ЦКБ ПЕК нормативно-правових актів та інших документів;
    б) розробляє та бере участь у розробленні проектів актів та інших документів з питань діяльності ЦКБ ПЕК, контролює відповідність документації законодавству;
    в) бере участь у підготовці та укладанні господарських та інших договорів з підприємствами, установами, організаціями;
    г) інші роботи в рамках діяльності Відділу.

- відстеження поточного стану нормативно-правової бази України в галузі інформаційної безпеки;
- оформлення результатів розслідувань кіберінцидентів згідно нормативних вимог.

4.2.3 Типові категорії (ролі) працівників Центрів

Типовими ролями співробітників ЦКБ можна визначити наступні:

- оператор (Call-Center, моніторинг, оперативне реагування на кіберінциденти);
- адміністратор (адміністрування системи та налаштування програмного забезпечення);
- аналітик (аналіз шкідливого програмного забезпечення, розвідка загроз);
- керівник (менеджер) (координація дій між користувачами ЦКБ).

4.2.4 Керівні документи

Набір основних документів, що регламентують роботу працівників ЦКБ:

1) посадові інструкції;
2) типові інструкції щодо алгоритмів дій у штатних та позаштатних ситуаціях;
3) політика управління інцидентами;
4) база даних про інциденти.

Необхідно передбачити впровадження політики безпеки на основі ролей, за якою автентифікація та авторизація виконуються на рівні центральної служби автентифікації та авторизації, тим самим обмежуючи доступ користувачів до даних та інструментів на основі ролей.

Всі спроби користувачів отримати доступ до користування послугами повинні бути зареєстровані з метою їх подальшої перевірки.

4.2.5 Розмежування доступу до ресурсів та функції

За рівнем повноважень щодо доступу до інформації персонал, який має доступ на ЦКБ ПЕК, поділяється на наступні категорії:

«Системний адміністратор» – виконує функції:

- адміністрування операційних систем (ОС) серверів та АРМів користувачів;
- адміністрування систем віртуалізації;
- створення, резервування/відновлення та видалення віртуальних серверів;
- встановлення, архівація, резервне копіювання та відновлення системного програмного забезпечення після програмних та/або апаратних збоїв;
- моніторинг працездатності та оновлення версій системного програмного забезпечення;
- забезпечення працездатності мережних сервісів, ведення політик безпеки та управління доступом до серверів і загальних сервісів;
- управління локальною та розподіленою мережею для доступу користувачів до ресурсів системи;
- технічне обслуговування серверів та робочих станцій;
- встановлення та налаштування антивірусного та спеціалізованого ПЗ.

«Адміністратор безпеки» – виконує функції:

- загальний контроль за станом безпеки;
- контроль відповідності налаштувань програмних та технічних засобів прийнятій політиці безпеки;
- реєстрація нових користувачів та видалення старих користувачів;
- призначення атрибутів доступу користувачів та об’єктів захисту;
- надання/обмеження користувачам прав доступу до об’єктів захисту згідно з їх повноваженнями;

- аудит подій щодо автентифікації і авторизації користувачів в ЦКБ ПЕК, доступу до об’єктів захисту, а також обробка та аналіз зареєстрованої інформації про критичні, з погляду безпеки події.
- налаштування параметрів безпеки серверів та АРМів користувачів;
- контроль виконання користувачами та адміністраторами вимог до захисту інформації
- установка та налаштування параметрів СКБД;
- архівація, резервне копіювання та відновлення баз даних та програмного забезпечення СКБД після програмних та/або апаратних збоїв;
- налаштовування параметрів резервного копіювання баз даних та програмного забезпечення СКБД;
- діагностика цілісності баз даних системи;
- керування антивірусним та спеціалізованим ПЗ захисту.

«Адміністратор ресурсів» – виконує функції:

- доступ до технологічної інформації окремих інформаційних ресурсів ЦКБ ПЕК: створення (видалення) та керування обліковими записами користувачів відповідного ресурсу ІТС;
- керування правами доступу та повноваженнями користувачів до об’єктів захисту відповідного ресурсу;
- налаштування відповідних сервісів ЦКБ ПЕК (відповідно до своїх повноважень);
- моніторинг роботи відповідного ресурсу за роботою системи (контроль роботи користувачів у системі).

«Звичайні користувачі» – для доступу до інформації у відповідності до своїх повноважень.

4.2.6 Вимоги до кваліфікації, навичок та навчання персоналу

Досвідчені аналітики (оператори моніторингу) мають бути здатні виконувати всі або більшість з наступних дій:

- виявляти потенційні вторгнення з начебто доброякісних наборів журналів аудиту або сигналів IDS;
- розробляти нові інструменти та методи для автоматизації трудомістких задач;
- збирати розрізнені дані (наприклад, системні журнали або образи жорстких дисків), будувати часову шкалу подій та оцінювати положення потенційного вторгнення;
- вміти інтерпретувати значення та належність показників трафіку за всіма рівнями стеку мережевих протоколів Open Source Interconnection (OSI) за допомогою інструментів аналізу мережевих протоколів;
- фрагментувати шкідливе ПЗ та формулювати робоче розуміння вектору атаки;
- виявляти некоректні конфігурації систем та взаємодіяти з відповідальними особами з метою усунення вразливостей;
- встановлювати та розвивати відносини з іншими представниками SOC суб'єктів CyberNet та CyberCenter для обміну провідним досвідом, інструментами та напрацюваннями;
- вміти моделювати поведінку супротивника, критично оцінювати структуру мережі, її функції та виявляти її слабкі місця шляхом тестування на проникнення.

Оператори та аналітики мають володіти додатковими якостями:

- наявність сильної інтуїції та здатність мислити «нестандартно»;
- увага до деталей при здатності зберігати бачення загальної картини;
- вміння підбирати нові концепції, прагнення до нових знань;
- бажання створювати сценарії та автоматизувати частини роботи, що повторюються.

4.2.6.1 Вимоги до кваліфікації

Кваліфікація персоналу має охоплювати знання в галузі інформаційних технологій та кібербезпеки, а також глибокі знання в як найменш одній або двох галузях, пов'язаних із захистом комп'ютерних мереж:

- формальне навчання в галузі інформаційних технологій, комп’ютерних наук, електротехніки та обчислювальної техніки, кібербезпеки або суміжних галузей;
- досвід роботи в галузі IT-операцій, системного/мережевого адміністрування або розробки програмного забезпечення;
- самостійне навчання системному адмініструванню, кодуванню програмного забезпечення, захисту комп’ютерних мереж, оцінці вразливостей, тестуванню на проникнення, яке виконується у вільний час кандидатів.

4.2.6.2 Вимоги до навичок

Оператори та аналітики повинні вміти працювати в наступних сферах:

- системне адміністрування Linux/UNIX, а також адміністрування мережі (маршрутизатор та комутатор), веб-серверів, брандмауерів або DNS;
- робота з різними інструментами FOSS IDS/IPS, NetFlow та інструментами збирання та аналізу протоколів, такими як Snort, Suricata, Bro, Argus, SiLK, tcpdump та WireShark;
- знання всього стеку мережевих протоколів TCP / IP або OSI, основні протоколи (IP, ICMP, TCP, UDP, SMTP, POP3, HTTP, FTP) включно та SSH;
- робочі знання поширених алгоритмів та протоколів криптографії, таких як Advanced Encryption Standard (AES), Rivest, Shamir & Adleman (RSA), алгоритм дайджеста повідомлень (MD5), алгоритм Secure Hash (SHA), Kerberos, Secure Socket Layer / Transport Layer Security (SSL / TLS), а також криптографічний протокол Diffe Hellman;
- проектування безпеки та архітектури – аналіз та розробка функцій безпеки більшості розподілених систем;

- робота з інструментами COTS NIDS / NIPS або HIDS / HIPS, такими як McAfee IntruShield та ePolicy Orchestrator (EPO), або Hewlett-Packard (HP) TippingPoint;
- робота з різними інструментами агрегації журналів та SIEM, такими як ArcSight або Splunk;
- досвід роботи з інструментами оцінки вразливостей та тестування на проникнення, такими як Metasploit, CORE Impact, Immunity Canvas або Kali Linux.
- досвід роботи з мовами програмування та скриптами, а також інструментами для роботи з текстом (Perl, sed та awk, grep, Ruby та Python).

Для аналітиків шкідливого коду додатково:

- знання асемблерного коду в Intel x86 та інших поширених архітектур;
- робота з інфраструктурами аналізу шкідливого коду, такими як ThreatTrack ThreatAnalyzer та FireEye AX;
- робота з допоміжними утилітами аналізу шкідливого коду (такими як SysInternals) та набором інструментів для декомпіляції та перевірки шкідливих програм (такими як IDA Pro).

Аналітики Відділу розслідувань кіберзагроз додатково:

- знати внутрішні компоненти Windows та інших поширених ОС, поширені файлові системи;
- інструменти експертизи та аналізу, такі як AccessData FTK або EnCase Forensic.

4.2.6.3 Вимоги до soft-навичок

- Письмове та мовленнєве спілкування;
- Здатність розвиватися у швидкому темпі та за стресових умов;
- Сильні риси командного гравця;
- Здатність забезпечити навчання на робочому місці та обмін знаннями з іншими аналітиками.

– Самостійна ініціатива з сильним тайм-менеджментом;
– Розуміння цілісності та ідентифікація з місією CyberNet та CyberCenter.

4.2.6.4 Вимоги до навчання персоналу

При організації робочого процесу з метою підвищення його ефективності та більш швидкої адаптації персоналу до умов праці рекомендується розробка власних навчальних програм, спрямованих на ознайомлення з основними цілями та задачами роботи Центрів, їх взаємодії з іншими Центрами галузі, програмним та апаратним забезпеченням, політиками системи менеджменту інформаційної безпеки та іншими нормативними та регламентними документами.

Відповідальність за планування, організацію, впровадження та контроль за виконанням наведених вище вимог покладається на відділ організації інформування та навчання суб'єктів CyberNet у CyberCenter.

4.3 Автоматизована телефонна система визначення рівня КІБ

В рамках дисертаційної роботи була захищена випускна кваліфікаційна робота магістерки Янко Анастасії Ігорівни групи МПІп-171 2017-2019 р.н. за темою «Створення автоматизованої телефонної системи для визначення рівня культури інформаційної безпеки компаній».

В роботі розглянуто проектування майбутньої системи визначення рівня культури безпеки організації, використовуючи нечітку логіку та методології визначення рівня КІБ, розглянутих попередньо.

На рисунку 4.12 представлено діаграму IDEF0, що сформована для визначення та ілюстрації необхідних компонентів у створенні автоматизованої телефонної системи, зібраних у ході розгляду попередніх розділів.

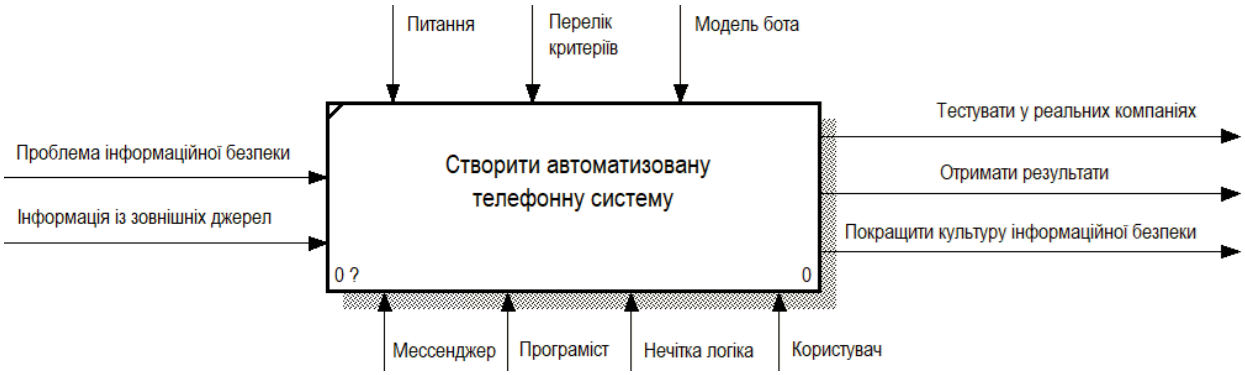

Рисунок 4.13 – Діаграма IDEF0 для автоматизованої телефонної системи

Схема збору даних та їх безпосередня обробка у додатку представлена на рисунку 4.13.

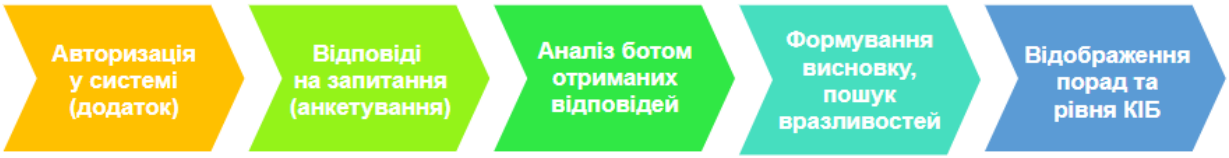

Рисунок 4.14 – Модель автоматизованої телефонної системи (розроблено автором ВКР)

Запропонована система функціонує у вигляді так званого чат-боту, додатку до будь-якого месенджера (наприклад, Telegram – за вибором автора ВКР), імітує поведінку людини, задаючи користувачу запитання. Взаємодія відбувається між додатком та користувачем. Рисунок 4.14 демонструє діаграму варіантів використання для АТС.

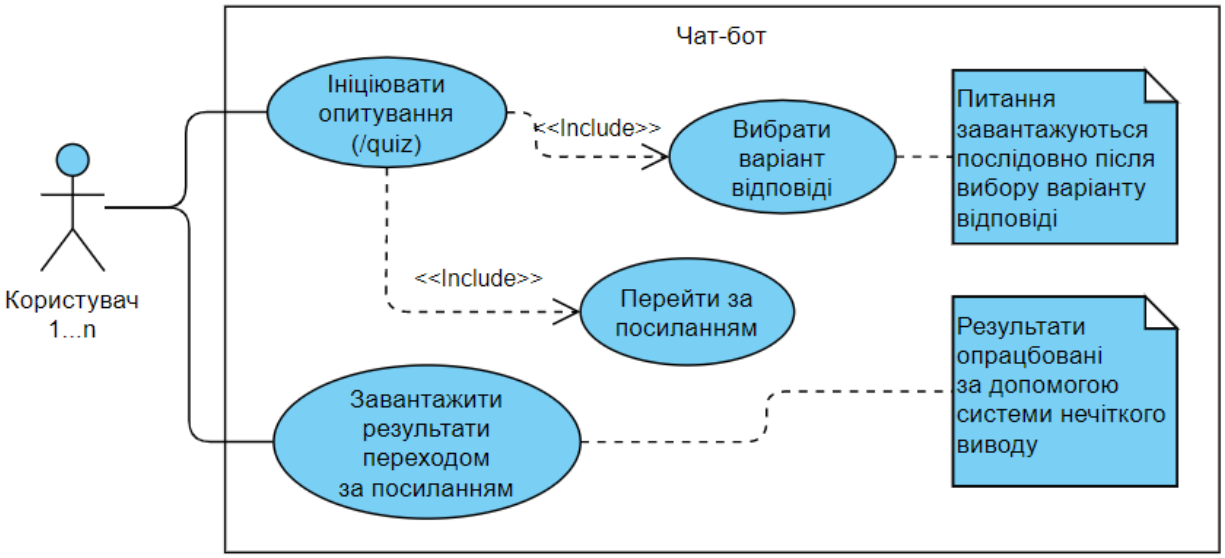

Рисунок 4.15 – Діаграма взаємодії для автоматизованої телефонної системи

Система визначення рівня КІБ містить у собі наступні компоненти:

– інтерфейс користувача;
– оброблювач вхідних даних;
– база правил системи нечіткого логічного виводу;
– оброблювач вихідних даних.

Робота чат-бота передбачає авторизацію користувача. Сигналом для початку опитування виступає команда «/quiz», введена за допомогою клавіатури. Алгоритм роботи з чат-ботом приведений на рисунку 4.15.

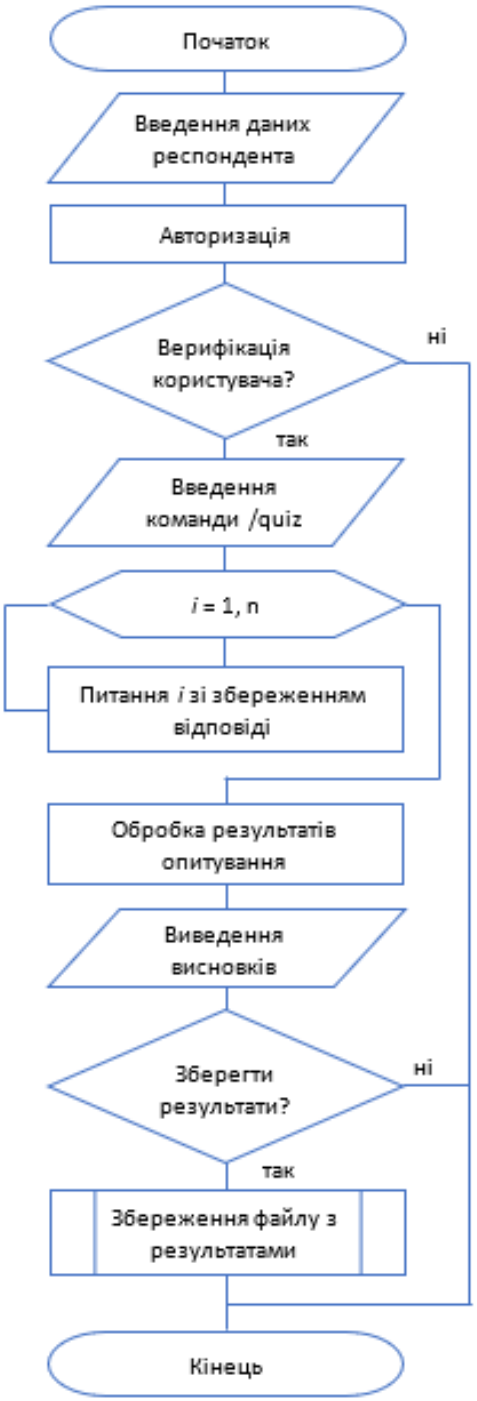

Рисунок 4.16 – Алгоритм роботи з чат-ботом

Бот по черзі виводить питання, що сформовані для визначення персональної КІБ (додаток Б), та пропонує декілька варіантів відповідей. Користувач вибирає відповідь, яку він вважає найбільш прийнятною для нього. Згідно до обраних відповідей оброблювач вихідних даних формує висновок про рівень персональної КІБ та надає його користувачу. Відповіді

формуються на основі бази правил СНВ. Це суттєво полегшує виведення результатів, а також внесення змін до БП.

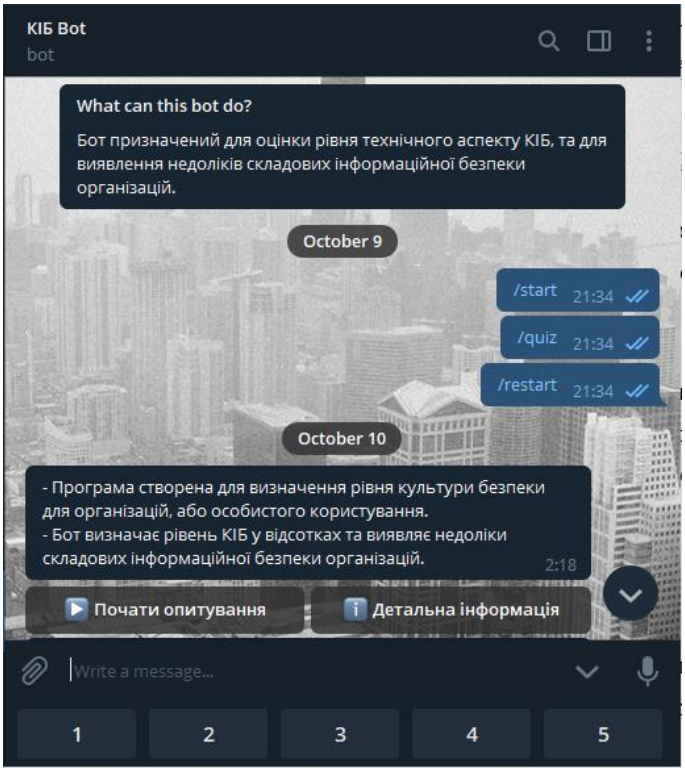

Рисунок 4.17 – Інтерфейс чат-бота

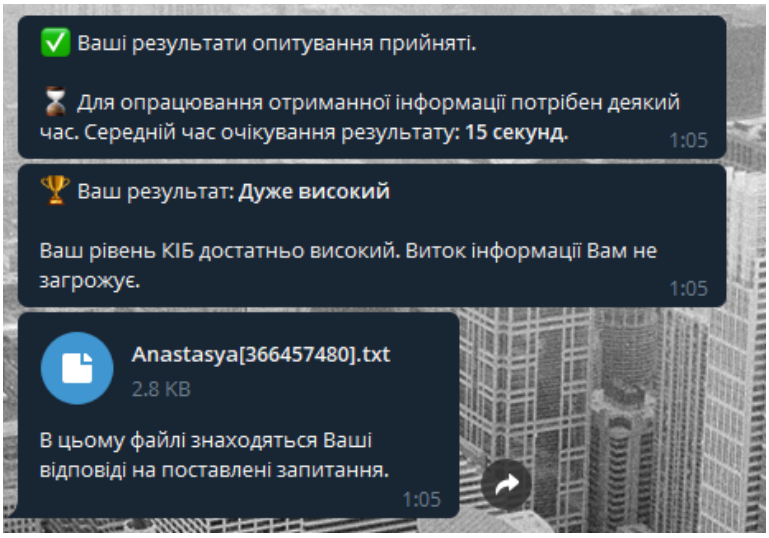

Рисунок 4.18 – Відображення результатів тестування

Використання чат-боту дозволяє проводити самооцінювання рівня персональної КІБ. Результати тестування з рекомендаціями пропонуються до завантаження у файлі формату .txt.

Висновки до розділу 4

За результатами практичного впровадження запропонованих моделей та методів можна зробити наступні висновки.

1. Елементи запропонованої інформаційної технології отримали перевірку у вигляді проведеного збору первинної інформації шляхом анкетування з використанням хмарних сервісів. Така форма опитування дозволила створити і загальні, і індивідуальні набори питань, що спрямовані на висвітлення певних аспектів ІБ у професійній діяльності працівників.
2. Отримані результати були опрацьовані за допомогою запропонованої нечіткої моделі оцінки персонального рівня КІБ, що виявило «вузькі місця» у системі інформаційної безпеки аспектів людино-машинної взаємодії в рамках бізнес-процесів організації. Це дозволило запропонувати рекомендації щодо підвищення рівня персональної культури інформаційної безпеки.
3. Після проведеного навчання результати повторного анкетування показали підвищення рівня персональної КІБ учасників: частка опитуваних, рівень КІБ яких був оцінений як «прийнятний захист» зросла з 21,05% до 34,21% за рахунок підвищення рівня обізнаності представників групи, рівень яких раніше був оцінений як «неприйнятий захист».
4. При виконанні робіт в рамках проекту «Розвиток базового моделюючого комплексу мережі ситуаційних центрів державних органів сектору безпеки і оборони України в інтересах захисту критичної інфраструктури держави та кібербезпеки» були сформовані моделі ІБ-компетенцій для персоналу суб’єктів CyberNet у CyberCenter, їх посадові обов’язки та вимоги, що формує вхідні характеристики для автоматизованої системи оцінки рівня КІБ організації.

5. Розроблений чат-бот забезпечує самооцінювання персонального рівня КІБ з подальшими результатами та рекомендований до використання у невеликих організаціях, які не мають можливостей проведення повного аудиту системи інформаційної безпеки.

Результати досліджень, приведених в розділі, опубліковані в роботах [72, 91].

ВИСНОВКИ

В результаті виконання дисертаційного дослідження сформульовано та вирішено актуальне наукове завдання щодо створення інформаційної технології оцінювання рівня культури інформаційної безпеки організації.

Актуальність дослідження підтверджується ретельним аналізом публікацій, який виявив необхідність формування методів та моделей інформаційної технології оцінювання рівня культури інформаційної безпеки організації з врахуванням персональних показників співробітників, актуальних ІБ-ризиків та нормативних вимог до ведення безпечної діяльності організації в умовах інформатизації.

За результатами дослідження можна зробити наступні висновки:

1. Сформований перелік первинних показників рівня культури інформаційної безпеки організації та її індикаторів, який враховує особливості професійної діяльності та специфікою взаємодії з інформаційною системою, внутрішнім інформаційним простором та зовнішнім середовищем, та ґрунтується на міжнародних стандартах ISO/IEC 27001:2015, ISO/IEC 27032:2016, а також напрацювань з методів та моделей формування культури безпеки на об’єктах критичної інфраструктури. Завдяки цьому дістала подальшого розвитку структура системи ІБ організації за рахунок включення факторів персональної КІБ, що дозволяє враховувати вплив людського чинника на загальну систему безпеки організації.
2. Розроблена модель інформаційного процесу оцінювання рівня культури інформаційної безпеки організації, яка на відміну від існуючих, містить аспекти людино-машинної взаємодії і враховує фактори персональної культури безпеки учасників процесу.
3. Розроблені елементи інформаційної технології визначення рівня культури інформаційної безпеки організації, які містять моделі і методи обрахування, базові елементи інформаційної системи (діаграми використання, послідовності, класів, а також архітектуру

та логічну модель бази даних), що складають основу методу автоматизованої оцінки рівня КІБ організації, який на відміну від існуючих, базується на використанні нечіткої логіки на основі алгоритму Мамдані, і дозволяє виконувати оцінку поетапно на різних організаційних рівнях. Також дістав подальшого розвитку метод оцінки рівня персональної КІБ на основі компетентнісного підходу за рахунок використання логіки антонімів, що забезпечує підвищення ефективності проведення таких оцінок.

4. Проведене експериментальне дослідження щодо збору та обробки первинної інформації для інформаційної технології оцінювання рівня культури інформаційної безпеки організації, та проведеного навчання дозволило підвищити показник рівня персональної КІБ з 21,05% до 34,21% та перейти з рівня «неприйнятий захист» до «прийнятного».

Практичне значення отриманих результатів полягає в тому, що наведені вище наукові результати у своїй сукупності утворюють нову інформаційну технологію оцінки рівня культури інформаційної безпеки організації. Запропонована інформаційна технологія може бути корисною для керівників ІБ-підрозділів та організацій для підтримки впроваджених систем забезпечення інформаційної безпеки. Розроблені бізнес-процеси та архітектура можуть бути використані як основа при розробці власних систем моніторингу культури інформаційної безпеки; модель оцінки персональної культури інформаційної безпеки – при призначенні певних рівнів доступу до інформаційних систем; моніторингу поточного рівня культури інформаційної безпеки персоналу, структурного підрозділу та, власне, організації для визначення прогалин в обізнаності та компетенцій в галузі ІБ; формуванні команд реагування на інциденти, тощо.

Результати дослідження можуть бути корисними для керівників ІБ-підрозділів та організацій для підтримки впроваджених систем забезпечення інформаційної безпеки. Розроблені бізнес-процеси та архітектура можуть бути

використані як основа для розроблення власних систем моніторингу культури інформаційної безпеки; модель оцінки персональної культури інформаційної безпеки – при призначенні певних рівнів доступу до інформаційних систем; моніторингу поточного рівня культури інформаційної безпеки персоналу, структурного підрозділу та саме організації для визначення прогалин в обізнаності та компетенцій в галузі ІБ; формуванні команд реагування на інциденти, тощо.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Резолюція, прийнята Генеральною Асамблеєю ООН 57/239. Створення глобальної культури кібербезпеки. 31 січня 2003 р. URL: http://www.ifap.ru/ofdocs/un/57239.pdf (дата звернення: 26.10.2018).

2. Про інформацію : Закон України від 02 жовтня 1992 № 2657-XII. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650. URL: https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12 (дата звернення: 26.10.2018).

3. Про рішення Ради національної безпеки і оборони України «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» : Указ Президента України від 28 квітня 2014 року №449/2014. *Офіційний вісник Президента України*. 2014. № 16. Ст. 982. URL: https://zakon.rada.gov.ua/laws/show/449/2014 (дата звернення: 26.10.2018).

4. Про рішення Ради національної безпеки і оборони України «Про нову редакцію Воєнної доктрини України» : Указ Президента України від 2 вересня 2015 року №555/2015. *Офіційний вісник Президента України*. 2015. № 22. Ст. 1291. URL: https://zakon.rada.gov.ua/laws/show/555/2015#n17 (дата звернення: 26.10.2018).

5. Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України» : Указ Президента України від 27 січня 2016 року № 96/2016. *Офіційний вісник України*. 2016. № 23. Ст. 899. URL: https://zakon5.rada.gov.ua/laws/show/96/2016 (дата звернення: 26.10.2018).

6. Про національну безпеку України : Закон України від 21 червня 2018 року № 2469-VIII. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 26.10.2018).

7. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України від 23.03.2007 №537-V. *Відомості Верховної Ради України*. 2007. № 12. Ст. 102 URL: https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=537-16 (дата звернення: 26.10.2018).

8. Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие. Москва – Берлин : Директ-Медиа, 2015. 253 с. URL: https://books.google.com.ua/books?id=yIo5CwAAQBAJ&printsec=frontcover&hl=ru#v=onepage&q&f=false (дата звернення: 26.10.2018).

9. Ліпкан В. А. Національна безпека України : навч. посіб. Київ : Кондор, 2008. 552 с. URL: http://pidruchniki.com/16850303/politologiya/ponyattya_zmist_informatsiynoyi_bezpeki (дата звернення: 26.10.2018).

10. Велігура А. В. Оцінювання стану інформаційної безпеки підприємства. *Управління проектами та розвиток виробництва* : зб. наук. пр. 2014. № 4(52). С. 28-39. URL: https://cyberleninka.ru/article/n/otsinyuvannya-stanu-informatsiynoyi-bezpeki-pidpriemstva (дата звернення: 26.10.2018).

11. Кобозева А. А., Хорошко В. А. Анализ информационной безопасности. Київ : Изд-во ГУИКТ, 2009. 251 с.

12. Шумейко О. О. Інформаційна безпека. Дніпродзержинськ : Дніпродзержинський державний технічний університет, 2012. 144 с. URL: http://www.dstu.dp.ua/Portal/Data/3/19/3-19-z_np4.pdf (дата звернення: 30.10.2018).

13. Атаманов Г. А. Агасофия информации : Природа информации. Информационная модель мира : монография / Федер. гос. авт. образоват. учреждение высш. образования «Волгогр. гос. ун-т». Волгоград : Изд-во ВолГУ, 2017. 122 с. URL: http://gatamanov.blogspot.com/2018/01/blog-post.html (дата звернення: 30.10.2018).

14. ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT).

15. Благовещенский А. Н., Благовещенский П. А. Основы организации системы обеспечения информационной безопасности для специальности «Прикладная информатика в экономике». *ОТО*. 2014. № 3. URL: https://cyberleninka.ru/article/n/osnovy-organizatsii-sistemy-obespecheniya-informatsionnoy-bezopasnosti-dlya-spetsialnosti-prikladnaya-informatika-v-ekonomike (дата звернення: 16.01.2020).

16. Развитие информационных угроз в третьем квартале 2017 года / АО Kaspersky Lab. URL: https://securelist.ru/it-threat-evolution-q3-2017/87961/ (дата звернення: 16.01.2018).

17. How to Assess Security Maturity and Make Improvements / Security Architects Partners. URL: https://security-architect.com/how-to-assess-security-maturity-and-roadmap-improvements/ (дата звернення: 15.07.2020).

18. Войцеховська М. М. Культурно-антропологічні чинники інформаційної безпеки в умовах постіндустріального суспільства. *Юність науки – 2017: соціально-економічні та гуманітарні аспекти розвитку суспільства :* Міжнародна науково-практична конференція студентів, аспірантів і молодих вчених (м. Чернігів, 25–27 квітня 2017 р.). Чернігів : ЧНТУ, 2017. С. 452-454.

19. Войцеховська М. М., Дорош М. С. Використання експертної системи на базі нечіткої логіки для визначення рівня культури інформаційної безпеки організації. *Проблеми зняття з експлуатації об'єктів ядерної енергетики та відновлення навколишнього середовища (INUDECO 18)* : збірник матеріалів III Міжнародної конференції (25-27 квітня 2018 року, м. Славутич). Чернігів : ЧНТУ, 2018. С. 61–64.

20. Дорош М. С., Войцеховська М. М. Впровадження культури інформаційної безпеки при управлінні проектами. *Безпека соціально-економічних процесів в кіберпросторі* : матеріали Всеукраїнської науково-практичної конференції ; 27 березня 2019 р. Київ : КНТЕУ, 2019. С. 175-176.

21. Дорош М. С., Войцеховська М. М., Дружинін О. О. Фактори безпеки при виборі інформаційних систем управління проектами. *Управління проектами у розвитку суспільства :* XVI Міжнародна конференція (м. Київ, 17-18 травня 2019 р.). Київ, 2019. С. 106-108.

22. Литвинов В. В., Трунова О. В., Войцеховська М. М. Формування і підвищення культури інформаційної безпеки організації. *Створення та модернізація озброєння і військової техніки в сучасних умовах :* Шістнадцята науково-технічна конференція. Чернігів, 2016. С. 163–164.

23. Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, 29(4), pp. 476–486. DOI: 10.1016/j.cose.2009.10.005.

24. Ngo, L., Zhou, W. & Warren, M. (2005). Understanding Transition towards Information Security Culture Change. Proceedings of *3rd Australian Information Security Management Conference* (2005), 67–73.

25. Furnell, S., & Thomson, K. L. (2009). From culture to disobedience: Recognising the varying user acceptance of IT security. *Computer Fraud and Security*, 2, pp. 5–10. DOI: 10.1016/S1361-3723(09)70019-3.

26. Da Veiga, a., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), pp. 196–207. DOI: 10.1016/j.cose.2009.09.002.

27. Flores, W., Antonsen, E. & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioural information security governance and national culture. *Computers & Security*, 43, pp. 90–110. DOI: 10.1016/j.cose.2014.03.004.

28. Schlienger, Thomas & Teufel, Stephanie. (2003). Information security culture: From analysis to change. *South African Computer Journal*, 31, pp. 46-52.

29. Alhogail, Areej & Mirza, A. (2014). A framework of information security culture change. *Journal of Theoretical and Applied Information Technology*, 64, pp. 540-549.

30. Sherif, Emad & Furnell, Steven & Clarke, Nathan. (2015). An Identification of Variables Influencing the Establishment of Information Security Culture. *Lecture Notes in Computer Science*. Springer, Cham. *International Conference on Human Aspects of Information Security, Privacy, and Trust. HAS 2015*, Vol. 9190, pp. 436-448. DOI: 10.1007/978-3-319-20376-8_39.

31. 2012 Data Breach QuickView. (2013). [online] Risk Based Security, Inc. Available at: https://www.riskbasedsecurity.com/reports/2012-DataBreachQuickView.pdf [Accessed 1 Feb. 2019].

32. 2013 Data Breach QuickView. (2014). [online] Risk Based Security, Inc. Available at: https://www.riskbasedsecurity.com/reports/2013-DataBreachQuickView.pdf [Accessed 1 Feb. 2019].

33. 2014 Year End Data Breach QuickView. (2015). [online] Risk Based Security, Inc. Available at: https://www.riskbasedsecurity.com/reports/2014-YEDataBreachQuickView.pdf [Accessed 1 Feb. 2019].

34. 2015 Year End Data Breach QuickView. (2016). [online] Risk Based Security, Inc. Available at: https://www.riskbasedsecurity.com/2015-data-breach-quickview [Accessed 1 Feb. 2019].

35. 2016 Year End Data Breach QuickView Report. (2017). [online] Risk Based Security, Inc. Available at: https://pages.riskbasedsecurity.com/2016-ye-breach-quickview [Accessed 1 Feb. 2019].

36. 2017 Q1 Data Breach Quick View Report. (2017). [online] Risk Based Security, Inc. Available at: https://pages.riskbasedsecurity.com/2017-q1-breach-quickview [Accessed 1 Feb. 2019].

37. 2017 MidYear Data Breach QuickView Report. (2017). [online] Risk Based Security, Inc. Available at: https://pages.riskbasedsecurity.com/2017-midyear-breach-quickview-report [Accessed 1 Feb. 2019].

38. 2017 Q3 Data Breach QuickView Report. (2017). [online] Risk Based Security, Inc. Available at: https://pages.riskbasedsecurity.com/2017-q3-breach-quickview-report [Accessed 1 Feb. 2019].

39. 2017 Year End Data Breach QuickView Report. (2018). [online] Risk Based Security, Inc. Available at: https://pages.riskbasedsecurity.com/2017-ye-breach-quickview-report [Accessed 1 Feb. 2019].

40. 2018 Q3 Data Breach QuickView Report. (2018). [online] Risk Based Security, Inc. Available at: https://pages.riskbasedsecurity.com/2018-q3-breach-quickview-report [Accessed 1 Feb. 2019].

41. Krombholz, K., Hobel, H., Huber, M., Weippl, E. (2013). Social engineering attacks on the knowledge worker. *Proceedings of the 6th International Conference on Security of Information and Networks* (pp. 28-35, November 26-28). Aksaray, Turkey. DOI: 10.1145/2523514.2523596.

42. Beugelsdijk, S., Maseland, R. (2010). *Culture in Economics: History, Methodological Reflections and Contemporary Applications*. Cambridge University Press.

43. Schlienger, Thomas & Teufel, Stephanie. (2002). Information Security Culture: The Socio-Cultural Dimension in Information Security Management. (pp. 191-202).

44. Francois Mouton, Louise Leenen, Venter H. S. (2016) Social engineering attack examples, templates and scenarios. *Computers and Security*, 59, pp. 186-209.

45. Okere I.; van Niekerk J.; Carroll M. (2012). Assessing information security culture: A critical analysis of current approaches. *Proceedings of the 2012 Information Security for South Africa* (pp. 1-8). DOI: 10.1109/ISSA.2012.6320442.

46. Alhogail. and A. Mirza. (2014). Information security culture: a definition and a literature review. *Proceedings of IEEE World Congress On Computer Applications and Information Systems* (pp. 1–7).

47. Paschal, A. Ochang, Philip, J. Irving, Paulinus, O. Ofem (2016). Research on Wireless Network Security Awareness of Average Users. *International*

Journal of Wireless and Microwave Technologies(IJWMT), 6(2), pp. 21-29. DOI: 10.5815/ijwmt.2016.02.03.

48. Толстова Ю. Н. Измерение в социологии : учебное пособие. Москва : КДУ, 2007. 288 с.: ил., табл. URL: https://socioline.ru/files/5/41/tolstova_yu.n._-_izmerenie_v_sociologii._uchebnoe_posobie_-_2007.pdf (дата обращения: 16.12.2017).

49. Культура безпеки в ядерній енергетиці : підручник / В. В. Бєгун та ін. Київ, 2012. 539 с.

50. Хромцов А. В. Социально-технологическая культура персонала, как фактор формирования конкурентноспособности фирмы. *Ломоносов-2007* : материалы конференции. URL: https://lomonosov-msu.ru/archive/Lomonosov_2007/17/hromcov_av.doc.pdf (дата обращения: 16.12.2017).

51. Rotvold, G. (Nov/Dec., 2008). How to Create a Security Culture in Your Organization. *Information Management Journal*. http://findarticles.com/p/articles/mi_qa3937/is_200811/ai_n31111129/?tag=content;col1.

52. Schlienger, T. and Teufel, S. (2003). Information Security Culture - From Analysis to Change. 3*rd Annual Information Security South Africa Conference,* Johannesburg, South Africa, ISSA: http://icsa.cs.up.ac.za/issa/2003/Publications.

53. Литвинов В. В., Трунова О. В., Войцеховська М. М. Модель культури інформаційної безпеки організації. *Перспективні напрями захисту інформації :* Друга всеукраїнська науково-практична конференція. Одеса, 2016. С. 47–50.

54. Adéle da Veiga, Nico Martins. (2017). Defining and identifying dominant information security cultures and subcultures, *Computers & Security,* 70, pp. 72-94. http://dx.doi.org/doi: 10.1016/j.cose.2017.05.002.

55. Dorosh, M., Trunova, O., Itchenko, D., Voitsekhovska, M., Dvoieglazova, M. (2016). The study of participants' values convergence on the example of international scientific project on cyber security. *Eastern-European Journal of Enterprise Technologies*, 6/3(84), pp. 4-10. DOI: 10.15587/1729-4061.2016.85215 (SCOPUS).

56. Shkarlet, S., Dorosh, M., Druzhynin, O., Voitsekhovska, M., Bohdan, I. (2021). Modeling of Information Security Management System in the Project. *MODS 2020. Advances in Intelligent Systems and Computing*. Springer, Cham. *P. II. Mathematical Modeling and Simulation of Systems,* 1265, pp. 364-376. DOI: 10.1007/978-3-030-58124-4_35 (SCOPUS).

57. Атаманов Г. А. О цене и ценности информации. *Защита информации. Инсайд*. 2016. № 6. С. 19–21. URL: http://gatamanov.blogspot.ru/2016/12/blog-post_20.html (дата обращения: 20.10.2019).

58. Пискунов И. Оценка стоимости информационных активов. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/informational_assessment#part5 (дата обращения: 20.10.2019).

59. Астахов А. М. Искусство управления информационными рисками. Москва : ДМК Пресс, 2010. 312 с. URL: https://books.google.com.ua/books?id=1lydDQAAQBAJ&printsec=frontcover&hl=ru#v=onepage&q&f=false (дата обращения: 20.10.2019).

60. Руководство по реагированию на инциденты информационной безопасности / АО Kaspersky Lab. URL: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/

03/07172131/Incident_Response_Guide_rus.pdf (дата обращения: 05.09.2018).

61. Руководство ASCOT. Руководство по самостоятельной оценке культуры безопасности и проведению миссии группы ASCOT. URL: https://www.sunpp.mk.ua/sites/default/files/documents/TecDoc743_ASCOT_rus.pdf (дата обращения: 05.09.2018).

62. Методика оценки уровня культуры безопасности на предприятиях ядерного топливного цикла" (РБ 047-08). URL: https://files.stroyinf.ru/Data1/55/55266/index.htm (дата обращения: 05.09.2018).

63. Методика и критерии оценки состояния культуры безопасности ГП НАЭК «Энергоатом». МТ-Д.0.03.486–09. Киев, 2009.

64. Доклад Международной консультативной группы по ядерной безопасности «Управление эксплуатационной безопасностью АЭС», INSAG-13, МАГАТЭ, Вена, 1999.

65. Ломаков Ю. А. Методики оценивания рисков и их программные реализации в компьютерных сетях. *Молодой ученый*. 2013. № 2. С. 43-46. URL: https://moluch.ru/archive/49/6279/ (дата обращения: 06.09.2018).

66. Risk & Compliance Management Software & Services. https://riskwatch.com. [Accessed 09 Sept. 2018].

67. «ГРИФ» программный комплекс анализа и контроля рисков информационных систем компаний. URL: http://sec4all.net/grif.html (дата обращения: 09.09.2018).

68. The CORAS Method http://coras.sourceforge.net/index.html [Accessed 09 Sept. 2018].

69. A qualitative risk analysis and management tool – CRAMM Zeki Yazar (GSEC, Version 1.3). https://www.sans.org/reading-room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm-83 [Accessed 09 Sept. 2018].

70. Средство оценки безопасности Microsoft Security Assessment Tool. URL: https://docs.microsoft.com/ru-ru/previous-versions/msdn10/cc185712(v=msdn.10) (дата обращения: 09.09.2018).

71. Oracle Crystal Ball. https://www.oracle.com/technetwork/middleware/crystalball/overview/crystal-ball-131398.pdf. [Accessed 09 Sept. 2018].

72. Дорош М. С., Войцеховська М. М. Визначення рівня персональної культури інформаційної безпеки як складової загального показника безпеки корпоративних мереж. *Інформаційні технології та взаємодії» (IT&I'2018) :* V Міжнародна науково-практична конференція (20-21 листопада 2018 року). Київ : КНУ ім. Т. Шевченка. С. 267-268.

73. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014; IDT).

74. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014; IDT).

75. Муромець Н. Є., Чорноус О. І. Основи менеджменту підприємств автомобільного транспорту : навчальний посібник. Донецьк : ВІК, 2006. 314 с. URL: http://polka-knig.com.ua/article.php?book=161&article=10802 (дата звернення: 08.07.2018).

76. Вагин В. Н., Головина Е. Ю., Загорянская А. А., Фомина М. В. Достоверный и правдоподобный вывод в интеллектуальных системах.

Москва : Физматлит, 2004. 704 с. URL: http://www.ngpedia.ru/pg2801080cKAMACc0003184549/ (дата обращения: 26.12.2018).

77. Федулов А. А., Федулов Ю. Г., Цыгичко В. Н. Введение в теорию статистически ненадежных решений. Москва : Изд-во «Статистика», 1979. 281 с. URL: http://www.ngpedia.ru/pg6010048qpOnu5a0013184549 (дата обращения: 26.12.2018).

78. Rashmi Ravindra Chaudhari, Sonal Pramod Patil (Feb. 2017). Intrusion Detection System: Classification, Techniques Anddatasets to Implement. *International Research Journal of Engineering and Technology (IRJET). 04*(02), pp. 1860-1866. https://www.irjet.net/archives/V4/i2/IRJET-V4I2366.pdf.

79. Мілян К. В., Грицюк Ю. І. Особливості використання мережі Інтернет для отримання конфіденційної інформації. *Науковий вісник НЛТУ України*. 2013. Вип. 23.4. С. 314-328.

80. Alam, Javed & Pandey, Dr. Manoj. (2014). Advance Cyber Security System using fuzzy logic. *Journal of Management & IT ACME*, 10, pp. 17-29. https://www.researchgate.net/publication/279917296_Advance_Cyber_Security_System_using_fuzzy_logic.

81. Sallam, Hany. (February 2015). Cyber Security Risk Assessment Using Multi Fuzzy Inference System. *International Journal of Engineering and Innovative Technology (IJEIT)*, *4*(8), pp. 13-19. https://pdfs.semanticscholar.org/95cc/3661fd194263e27f0055f9cbcb0375f19192.pdf.

82. Al-Ali, Mansour & AlMogren, Ahmad. (September 2017). Fuzzy logic methodology for cyber security risk mitigation approach. *Journal of Networking Technology, 8*(3), pp. 83-90. http://www.dline.info/jnt/fulltext/v8n3/jntv8n3_2.pdf.

83. Zadeh, L. A. (1978). Fuzzy sets as basis for a theory of possibility. *Fuzzy Sets and Systems,* 1, pp. 3-28.

84. Aditya Pratap Singh, Pradeep Tomar. (2016). Web Service Component Reusability Evaluation: A Fuzzy Multi-Criteria Approach. *International Journal of Information Technology and Computer Science(IJITCS), 8*(1), pp. 40-47. DOI: 10.5815/ijitcs.2016.01.05.

85. Ashish Kumar Khare, J. L. Rana, R. C. Jain. (2017). Detection of Wormhole, Blackhole and DDOS Attack in MANET using Trust Estimation under Fuzzy Logic Methodology. *International Journal of Computer Network and Information Security (IJCNIS), 9*(7), pp. 29-35. DOI: 10.5815/ijcnis.2017.07.04.

86. Hany F. Atlam, Ahmed Alenezi, Raid Khalid Hussein, Gary B. Wills. (2018). Validation of an Adaptive Risk-based Access Control Model for the Internet of Things. *International Journal of Computer Network and Information Security (IJCNIS), 10*(1), pp. 26-35. DOI: 10.5815/ijcnis.2018.01.04.

87. Пегат А. Нечеткое моделирование и управление = Fuzzy modeling and control. 2-е изд. / пер. с англ. А. Г. Подвесовского, Ю. В. Тюменцева. Москва : Бином. Лаборатория знаний, 2013. 798 с. URL: http://padaread.com/?book=89681&pg=1 (дата обращения: 20.10.2018).

88. Sivanandam, S. N., Sumathi S., Deepa S. N. (Springer, 2007). Introduction to fuzzy logic using MATLAB.

89. Штовба С. Д. Введение в теорию нечетких множеств и нечеткую логику. MATLAB. Exponenta. URL: http://matlab.exponenta.ru/fuzzylogic/book1/4_6.php (дата обращения: 20.10.2018).

90. Войцеховська М. М., Бальченко І. В. Застосування нечіткої ієрархічної системи для оцінки базової культури кібербезпеки користувача (Применение нечеткой иерархической системы для оценки базовой

культуры кибернетической безопасности пользователя). *Математичне та імітаційне моделювання систем. МОДС 2018* : Тринадцята міжнародна науково-практична конференція (25–29 червня 2018 р., Україна, м. Чернігів). Чернігів : ЧНТУ, 2018. С. 339-341.

91. Dorosh, M., Voitsekhovska, M., Balchenko, I. (2020). Research and Determination of Personal Information Security Culture Level Using Fuzzy Logic Methods. In Hu Z., Petoukhov S., Dychka I., He M. (eds.) *Advances in Computer Science for Engineering and Education II. ICCSEEA 2019. Advances in Intelligent Systems and Computing*, vol. 938. Springer, Cham, pp. 503-512. DOI https://doi.org/10.1007/978-3-030-16621-2_47.

92. Shkarlet, S., Lytvynov, V., Dorosh, M., Trunova, E., Voitsekhovska, M. (2020). The Model of Information Security Culture Level Estimation of Organization. In Palagin A., Anisimov A., Morozov A., Shkarlet S. (eds.) *Mathematical Modeling and Simulation of Systems. MODS 2019. Advances in Intelligent Systems and Computing*, vol. 1019. Springer, Cham, pp. 249-258. DOI https://doi.org/10.1007/978-3-030-25741-5_25.

93. Bellman, R. E., Zadeh, L. A. (1970). Decision-making in a fuzzy environment. Management Science, 17 (4), pp. 141-164. DOI: 10.1287/mnsc.17.4.B141.

94. Saaty, Thomas L. (2008-06). Relative Measurement and its Generalization in Decision Making: Why Pairwise Comparisons are Central in Mathematics for the Measurement of Intangible Factors – The Analytic Hierarchy/Network Process (PDF). *RACSAM (Review of the Royal Spanish Academy of Sciences, Series A, Mathematics)*, 102(2), pp. 251–318.

95. Fishburn, C. P. (1968). Utility theory. *Management Science. Theory Series*, *14*(5), pp. 335-378.

96. Dunn J.C. A Fuzzy Relative of the ISODATA Process and Its Use in Detecting Compact Well-Separated Clusters // Journal of Cybernetics. — 1973. — 17 сентября (т. 3, № 3). — С. 32–57. — ISSN 0022-0280. — DOI:10.1080/01969727308546046.

97. Bezdek, James C. (1981). *Pattern Recognition with Fuzzy Objective Function Algorithms*. Plenum Press, New York.

98. Штовба С. Д., Нагорна А. В. Логічне виведення за їєрархічними гібридними нечіткими базами знань. // *Обчислювальний інтелект :* матеріали II Міжнародної науково-технічної конференції (Черкаси, Україна, 14-17 травня 2013 р.). URL: https://www.researchgate.net/publication/280304246_LOGICNE_VIVEDENNA_ZA_IERARHICNIMI_GIBRIDNIMI_NECITKIMI_BAZAMI_ZNAN (дата звернення: 20.20.2018).

99. Miller, J. A. (1956). The Magical Number Seven, Plus or Minus Two. Some Limits on Our Capacity for Processing Information. *Psychological Review*, 101, pp. 343-352.

100. Жилин Д. М., Ткачук Л. Э. О применимости теории чанков к обучению химии. *Естественнонаучное образование: время перемен* : сборник / под общей ред. академика В. В. Лунина и проф. Н. Е. Кузьменко. Москва : Издательство Московского университета, 2014. С. 138-154. URL: http://www.chem.msu.su/rus/books/2014/science-education-2014/138.pdf (дата обращения: 20.10.2018).

101. Saaty, T. L. (2008). Decision making with the analytic hierarchy process. *Int J Serv Sci,* 1(1), pp. 83-97. https://doi.org/10.1016/0270-0255(87)90473-8.

102. Трунова О. Застосування методу Сааті при прийнятті управлінських рішень. Вісник Чернігівського національного педагогічного університету. *Педагогічні науки*. 2013. Вип. 108.1. С. 130-137. URL:

http://nbuv.gov.ua/UJRN/VchdpuP_2013_1_108_34. (дата звернення: 11.03.2019).

103. Адаменко А. А., Ерошенко Я. Б., Кондрашова Т. В. Недетерминированные когнитивные модели на базе логики антонимов. *Научные ведомости Белгородского государственного университета. Серия: Экономика. Информатика.* 2014. Вып. 1-1 (172). Т. 29. С. 105-109. URL: http://cyberleninka.ru/article/n/nedeterminirovannye-kognitivnye-modeli-na-baze-logiki-antonimov (дата обращения: 11.03.2019).

104. Голота Я. Я. О формализации логики неполных знаний (логики антонимов). *Логика и развитие научного знания* : межвуз. сб. / под ред. И. Н. Бродского, Я. А. Слинина. Санкт-Петербург : СпбГУ, 1992. С. 92-112 (дата обращения: 15.04.2017).

105. Трунова О. В., Войцеховська М. М. Модель визначення рівня сформованості компетенцій ІТ-фахівця. *Математичне та імітаційне моделювання систем. МОДС 2017* : Дванадцята міжнародна науково-практична конференція (26-29 червня 2017 р., Україна, м. Чернігів). Чернігів : ЧНТУ, 2017. С. 376-378.

106. Трунова О. В., Войцеховська М. М. Використання логіки антонімів при оцінці стану культури інформаційної безпеки організації. *Проблеми зняття з експлуатації об'єктів ядерної енергетики та відновлення навколишнього середовища. INUDECO 2017* : матеріали ІІ Міжнародної конференції (м. Славутич, 25-27 квітня 2017). Чернігів, 2017. С. 276-280.

107. Войцеховська М. М. Логіка антонімів при оцінці компетенцій в галузі інформаційної безпеки. *Новітні технології у науковій діяльності і навчальному процесі* : Всеукраїнська науково-практична конференція

студентів, аспірантів та молодих вчених (м. Чернігів, 19–20 квітня 2017 р.). Чернігів : ЧНТУ, 2017. С. 47-48.

108. Половцев О. В. Лінгвістичні підходи до формалізації експертних оцінок в задачах державного управління. *Актуальні проблеми державного управління*. 2009. № 2. С. 42-50. URL: http://nbuv.gov.ua/UJRN/apdy_2009_2_7 (дата обращения: 10.04.2017).

109. Андрианов В. В., Зефиров С. Л., Голованов В. Б., Голдуев Н. А. Обеспечение информационной безопасности бизнеса. 2-е изд., перераб. и доп. Москва : Альпина Паблишерз, 2011. 373 с. URL: https://reader.bookmate.com/ygUDIFc0 (дата обращения: 18.04.2017).

110. Dorosh M., Voitsekhovska M. Information Security Culture Wide-Scale Implementation Model. *Проблеми зняття з експлуатації об'єктів ядерної енергетики та відновлення навколишнього середовища (INUDECO 20)* : збірник матеріалів IV Міжнародної конференції (27-29 квітня 2020 року, м. Славутич). Чернігів : ЧНТУ, 2020. С. 73-77.

111. Singh, Jagdeep & Singh, Harwinder. (2012). Continuous improvement approach: State-of-art review and future implications. *International Journal of Lean Six Sigma,* 3, pp. 88-111. DOI: 10.1108/20401461211243694.

112. Жемчугов А. М., Жемчугов М. К. Цикл PDCA Деминга. Современное развитие. *Проблемы экономики и менеджмента*. 2016. № 2. URL: http://corpsys.ru/articles/organization/deming-pdca-33.aspx (дата обращения: 10.03.2020).

113. Дубейковский В. И. Эффективное моделирование с AllFusion Process Modeler 4.1.4 и ALLFusion PM. Москва : Диалог-МИФИ, 2007. 382 с.

114. Lytvynov, V., Dorosh, M., Bilous, I., Voitsekhovska, M., Nekhai, V. (2020). Development of the automated information system for organization's

information security culture level assessment. *Technical sciences and technologies*, 1(19), pp. 124-132. DOI: 10.25140/2411-5363-2020-1(19)-124-132.

115. Про захист персональних даних : Закон України від 01 червня 2010 № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481. URL: https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2297-17 (дата звернення: 23.11.2019).

116. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовтня 2017 №2163-VIII. *Відомості Верховної Ради України.* 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/main/2163-19 (дата звернення: 23.11.2019).

117. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05 червня 1994 №80/94-ВР. *Відомості Верховної Ради України.* 1994. № 31. Ст. 286. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80 (дата звернення: 23.11.2019).

118. Про електронні документи та електронний документообіг : Закон України від 22 травня 2003 №851-IV. *Відомості Верховної Ради України*. 2003. № 36. Ст. 275. URL: https://zakon.rada.gov.ua/laws/show/851-15 (дата звернення: 23.11.2019).

119. ГСТУ СУІБ 2.0/ISO/IEC 27002:2010 «Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою» (ISO/IEC 27002:2005, MOD).

120. Дорош М. С., Нехай В. В., Войцеховська М. М. Архітектура інформаційної системи оцінки рівня культури інформаційної безпеки організації. *Математичне та імітаційне моделювання систем. МОДС 2019 :* Чотирнадцята міжнародна науково-практична конференція (24–26 червня 2019 р., Україна, м. Чернігів). Чернігів : ЧНТУ, 2019. С. 309-313.

121. Токарев Б. Принципы составления опросников для маркетологических исследований. URL: https://www.marketing.spb.ru/lib-research/methods/poll_questionnaire.htm (дата обращения: 08.10.2018).

122. Carson Zimmerman (2014). Ten Strategies of a World-Class Cybersecurity Operations Center. *The MITRE Corporation* (pp. 346). https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf.

ДОДАТКИ

ДОДАТОК А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Dorosh M., Trunova O., Itchenko D., Voitsekhovska M., Dvoieglazova M. The study of participants' values convergence on the example of international scientific project on cyber security. *Eastern-European Journal of Enterprise Technologies*, 2016. – Vol. 6/3 (84). – P. 4-10. DOI: 10.15587/1729-4061.2016.85215 (SCOPUS).
2. Dorosh M., Voitsekhovska M., Balchenko I. Research and Determination of Personal Information Security Culture Level Using Fuzzy Logic Methods. *Advances in Intelligent Systems and Computing*. Springer, Cham. *P. II : Advances in Computer Science for Engineering and Education.* – 2020. – Vol. 938. – P. 503–512. DOI https://doi.org/10.1007/978-3-030-16621-2_47 (SCOPUS, SpringerLink).
3. Shkarlet S., Lytvynov V., Dorosh M., Trunova E., Voitsekhovska M. The Model of Information Security Culture Level Estimation of Organization. *Advances in Intelligent Systems and Computing*. Springer, Cham. *P. II.* : *Mathematical Modeling and Simulation of Systems*. – 2020. – Vol. 1019. – P. 249-258. DOI https://doi.org/10.1007/978-3-030-25741-5_25 (SCOPUS, SpringerLink).
4. Lytvynov V., Dorosh M., Bilous I., Voitsekhovska M., Nekhai V. Development of the automated information system for organization's information security culture level assessment. *Technical sciences and technologies*. 2020. № 1 (19). P. 124-132. DOI: 10.25140/2411-5363-2020-1(19)-124-132.
5. Shkarlet S., Dorosh M., Druzhynin O., Voitsekhovska M., Bohdan I. (2021) Modeling of Information Security Management System in the Project. *MODS 2020. Advances in Intelligent Systems and Computing*. Springer, Cham. *P. II. Mathematical Modeling and Simulation of Systems.* – 2021. – Vol. 1265. –

P. 364-376. DOI https://doi.org/10.1007/978-3-030-58124-4_35 (SCOPUS, SpringerLink).

Наукові праці, які засвідчують апробацію матеріалів дисертації:

6. Литвинов В.В., Трунова О.В., Войцеховська М.М. Модель культури інформаційної безпеки організації. *Перспективні напрями захисту інформації* : зб. тез доп. другої Всеукр. наук.-практ. конф. (м. Одеса, 03-07 верес. 2017 р.). - Одеса, 2016. – С. 47-50.
7. Литвинов В.В., Трунова О.В., Войцеховська М.М. Формування і підвищення культури інформаційної безпеки організації. *Створення та модернізація озброєння і військової техніки в сучасних умовах* : зб. тез доп. шістнадцятої наук.-тех. конф. (м. Чернігів, 08-09 верес. 2016 р.). – Чернігів, 2016. – С. 163-164.
8. Трунова О.В., Войцеховська М.М. Використання логіки антонімів при оцінці стану культури інформаційної безпеки організації. *Проблеми зняття з експлуатації об'єктів ядерної енергетики та відновлення навколишнього середовища INUDECO 2017* : матеріали другої Міжнар конференції (м. Славутич, 25-27 квіт. 2017 р.). – Славутич, 2017. – С. 276-280.
9. Войцеховська М.М. Культурно-антропологічні чинники інформаційної безпеки в умовах постіндустріального суспільства. *Юність науки – 2017: соціально-економічні та гуманітарні аспекти розвитку суспільства* : зб. тез доп. Міжнар. наук.-практ. конф. студ., аспір. і молод. вчених (м. Чернігів, 25-27 квіт. 2017 р.). – Чернігів : ЧНТУ, 2017. – С. 452-454.
10. Войцеховська М.М. Логіка антонімів при оцінці компетенцій в галузі інформаційної безпеки. *Новітні технології у науковій діяльності і навчальному процесі* : зб. тез доп. Всеукр. наук.-практ. конф. студ., аспір. та молод. вчених (м. Чернігів, 19-20 квіт. 2017 р.) – Чернігів : ЧНТУ, 2017. – С. 47-48.

11. Трунова О.В., Войцеховська М.М. Модель визначення рівня сформованості компетенцій ІТ-фахівця. *Математичне та імітаційне моделювання систем. МОДС 2017* : зб. тез доп. дванадцятої Міжнар. наук.-практ. конф. (м. Чернігів, 26-29 черв. 2017 р.) – Чернігів : ЧНТУ, 2017. – С. 376-378.
12. Войцеховська М. М., Дорош М. С. Використання експертної системи на базі нечіткої логіки для визначення рівня культури інформаційної безпеки організації. *Проблеми зняття з експлуатації об'єктів ядерної енергетики та відновлення навколишнього середовища (INUDECO 2018)* : зб. матеріалів ІІІ Міжнар. конф. (м. Славутич, 25-27 квіт. 2018 р.). – Чернігів : ЧНТУ, 2018. – С. 61-64.
13. Войцеховська М.М., Бальченко І.В. Застосування нечіткої ієрархічної системи для оцінки базової культури кібербезпеки користувача (Применение нечеткой иерархической системы для оценки базовой культуры кибербезопасности пользователя). *Математичне та імітаційне моделювання систем. МОДС 2018* : зб. тез доп. тринадцятої Міжнар. наук.-практ. конф. (м. Чернігів, 25-29 червня 2018 р.). – Чернігів : ЧНТУ, 2018. – С. 339-341.
14. Дорош М.С., Войцеховська М.М. Визначення рівня персональної культури інформаційної безпеки як складової загального показника безпеки корпоративних мереж. *Інформаційні технології та взаємодії (IT&I'2018)* : зб. тез доп. V Міжнар. наук.-практ. конф. (м. Київ, 20-21 листоп. 2018 р.). – Київ : КНУ ім. Т. Шевченка, 2018. –С. 267-268.
15. Дорош М.С., Войцеховська М.М. Впровадження культури інформаційної безпеки при управлінні проектами. *Безпека соціально-економічних процесів в кіберпросторі* : матеріали Всеукр. наук.-практ. конф. (м. Київ, 27 берез. 2019 р.) – Київ : КНТЕУ, 2019. – С. 175-176.
16. Дорош М.С., Войцеховська М.М., Дружинін О.О. Фактори безпеки при виборі інформаційних систем управління проектами. *Управління*

проектами у розвитку суспільства : матеріали XVI міжнар. конф. (м. Київ, 17-18 трав. 2019 р.). – Київ, 2019. –С. 106-108.

17. Дорош М.С., Нехай В.В., Войцеховська М.М. Архітектура інформаційної системи оцінки рівня культури інформаційної безпеки організації. *Математичне та імітаційне моделювання систем. МОДС 2019* : зб. тез доп. Чотирнадцятої міжнар. наук.-практ. конф. (м. Чернігів, 24-26 черв. 2019 р.). – Чернігів : ЧНТУ, 2019. –С. 309-313.
18. Dorosh M., Voitsekhovska M. Information Security Culture Wide-Scale Implementation Model. *Проблеми зняття з експлуатації об'єктів ядерної енергетики та відновлення навколишнього середовища (INUDECO 2020)* : зб. матеріалів IV Міжнар. конф. (м. Славутич, 27-29 квітня 2020 р.). – Чернігів : ЧНТУ, 2020. – С. 73-77.

ДОДАТОК Б

Таблиця Б.1 – Приклад анкети

Назва змінної			Питання	Варіанти відповідей	Терм	Функція належності
Результуюча	Проміжна	Вхідна				
1	2	3	4	5	6	7
y_4	y_1	x_1	Акаунти для роботи та інтересів	Я користуюсь одним акаунтом, ноутбуком та смартфоном, ціную мобільність та переваги синхронізації	L	$\mu_L(x_1)=\begin{cases}1, & x_1\le 1\\ 2-x_1, & 1\le x_1\le 2\\ 0, & x_1\ge 2\end{cases}$
				Грань між робочими й особистими гаджетами дуже умовна, але я намагаюся їх розділяти	M	$\mu_M(x_1)=\begin{cases}0, & x_1\le 1\\ x_1-1, & 1\le x_1\le 2\\ 3-x_1, & 2\le x_1\le 3\\ 0, & x_1\ge 3\end{cases}$
				Використовую робочий ноутбук, телефон і окрему поштову адресу	H	$\mu_H(x_1)=\begin{cases}0, & x_1\le 2\\ x_1-2, & 2\le x_1\le 3\\ 1, & x_1\ge 3\end{cases}$
		x_2	Обліковий запис в операційній системі	Працюю під обліковим записом адміністратора. Дратують обмеження прав доступу	M	$\mu_M(x_2)=\begin{cases}0, & x_2\le 1\\ x_2-1, & 1\le x_2\le 2\\ 3-x_2, & 2\le x_2\le 3\\ 0, & x_2\ge 3\end{cases}$
				Працюю під особистим обліковим записом в якості користувача	H	$\mu_H(x_2)=\begin{cases}0, & x_2\le 2\\ x_2-2, & 2\le x_2\le 3\\ 1, & x_2\ge 3\end{cases}$
				Не бачу необхідності у створенні акаунта	L	$\mu_L(x_2)=\begin{cases}1, & x_2\le 1\\ 2-x_2, & 1\le x_2\le 2\\ 0, & x_2\ge 2\end{cases}$
		x_3	Активність у соціальних мережах	Є облікові записи в основних мережах. Полюбляю викладати фото і ділитися враженнями з друзями	L	$\mu_L(x_3)=\begin{cases}1, & x_3\le 1\\ 2-x_3, & 1\le x_3\le 2\\ 0, & x_3\ge 2\end{cases}$
				Моя персональна сторінка для цікавих приміток, музики та відео	ML	$\mu_{ML}(x_3)=\begin{cases}0, & x_3\le 1\\ x_3-1, & 1\le x_3\le 2\\ 3-x_3, & 2\le x_3\le 3\\ 0, & x_3\ge 3\end{cases}$
				Є акаунти, але рідко оновлюю свої сторінки	M	$\mu_M(x_3)=\begin{cases}0, & x_3\le 2\\ x_3-2, & 2\le x_3\le 3\\ 4-x_3, & 3\le x_3\le 4\\ 0, & x_3\ge 4\end{cases}$
				Акаунти були, проте зник інтерес до відвідування соцмереж	MH	$\mu_{MH}(x_3)=\begin{cases}0, & x_3\le 3\\ x_3-3, & 3\le x_3\le 4\\ 5-x_3, & 4\le x_3\le 5\\ 0, & x_3\ge 5\end{cases}$
				Ніколи не був(ла) зареєстрований(а) у соцмережах	H	$\mu_H(x_3)=\begin{cases}0, & x_3\le 4\\ x_3-4, & 4\le x_3\le 5\\ 1, & x_3\ge 5\end{cases}$
	y_2	x_4	Оновлення операційної системи та програмного забезпечення	Використовую автоматичне оновлення. ОС і ПЗ оновлюються по мірі виходу оновлень	H	$\mu_H(x_4)=\begin{cases}0, & x_4\le 2\\ x_4-2, & 2\le x_4\le 3\\ 1, & x_4\ge 3\end{cases}$
				Встановлюю оновлення вручну та вибірково	M	$\mu_M(x_4)=\begin{cases}0, & x_4\le 1\\ x_4-1, & 1\le x_4\le 2\\ 3-x_4, & 2\le x_4\le 3\\ 0, & x_4\ge 3\end{cases}$
				Не завантажую оновлення: істотно не впливають на роботу комп'ютера	L	$\mu_L(x_4)=\begin{cases}1, & x_4\le 1\\ 2-x_4, & 1\le x_4\le 2\\ 0, & x_4\ge 2\end{cases}$
		x_5	Антивірусні програми	Встановлено на кожному обчислювальному пристрої	H	$\mu_H(x_5)=\begin{cases}0, & x_5\le 2\\ x_5-2, & 2\le x_5\le 3\\ 1, & x_5\ge 3\end{cases}$
				Встановлено на ноутбуці/комп'ютері	M	$\mu_M(x_5)=\begin{cases}0, & x_5\le 1\\ x_5-1, & 1\le x_5\le 2\\ 3-x_5, & 2\le x_5\le 3\\ 0, & x_5\ge 3\end{cases}$

Продовження Таблиці Б.1

1	2	3	4	5	6	7
				Антивірус не встановлено	L	$\mu_L(x_5)=\begin{cases}1, & x_5\le 1\\ 2-x_5, & 1\le x_5\le 2\\ 0, & x_5\ge 2\end{cases}$
		x_6	Сканування системи антивірусом	Один раз на тиждень	H	$\mu_H(x_6)=\begin{cases}0, & x_6\le 4\\ x_6-4, & 4\le x_6\le 5\\ 1, & x_6\ge 5\end{cases}$
				Один раз на два тижні	MH	$\mu_{MH}(x_6)=\begin{cases}0, & x_6\le 3\\ x_6-3, & 3\le x_6\le 4\\ 5-x_6, & 4\le x_6\le 5\\ 0, & x_6\ge 5\end{cases}$
				Один раз на місяць	M	$\mu_M(x_6)=\begin{cases}0, & x_6\le 2\\ x_6-2, & 2\le x_6\le 3\\ 4-x_6, & 3\le x_6\le 4\\ 0, & x_6\ge 4\end{cases}$
				Ще рідше	ML	$\mu_{ML}(x_6)=\begin{cases}0, & x_6\le 1\\ x_6-1, & 1\le x_6\le 2\\ 3-x_6, & 2\le x_6\le 3\\ 0, & x_6\ge 3\end{cases}$
				Ніколи (антивірус не встановлено)	L	$\mu_L(x_6)=\begin{cases}1, & x_6\le 1\\ 2-x_6, & 1\le x_6\le 2\\ 0, & x_6\ge 2\end{cases}$
	y_3	x_7	Онлайн-банкінг	Регулярно користуюся для оплати товарів та послуг	L	$\mu_L(x_7)=\begin{cases}1, & x_7\le 1\\ 2-x_7, & 1\le x_7\le 2\\ 0, & x_7\ge 2\end{cases}$
				Використовую дуже рідко	M	$\mu_M(x_7)=\begin{cases}0, & x_7\le 1\\ x_7-1, & 1\le x_7\le 2\\ 3-x_7, & 2\le x_7\le 3\\ 0, & x_7\ge 3\end{cases}$
				Віддаю перевагу звичним грошовим відносинам	H	$\mu_H(x_7)=\begin{cases}0, & x_7\le 2\\ x_7-2, & 2\le x_7\le 3\\ 1, & x_7\ge 3\end{cases}$
		x_8	Блокування телефону і ноутбука	Використовую символьний або графічний блокувальник екрану	M	$\mu_M(x_8)=\begin{cases}0, & x_8\le 1\\ x_8-1, & 1\le x_8\le 2\\ 3-x_8, & 2\le x_8\le 3\\ 0, & x_8\ge 3\end{cases}$
				Використовую біометричний блокувальник екрану (відбиток пальця)	H	$\mu_H(x_8)=\begin{cases}0, & x_8\le 2\\ x_8-2, & 2\le x_8\le 3\\ 1, & x_8\ge 3\end{cases}$
				Не використовую блокувальник: це незручно і мені нема чого приховувати	L	$\mu_L(x_8)=\begin{cases}1, & x_8\le 1\\ 2-x_8, & 1\le x_8\le 2\\ 0, & x_8\ge 2\end{cases}$
				Мій телефон не має захисної функції блокування екрану	L	$\mu_L(x_8)=\begin{cases}1, & x_8\le 1\\ 2-x_8, & 1\le x_8\le 2\\ 0, & x_8\ge 2\end{cases}$
		x_9	Щодо паролів	Використовую окремий пароль для кожного облікового запису. Зберігаю їх у зручному місці (в записнику, в ящику столу, в окремому файлі)	MH	$\mu_{MH}(x_9)=\begin{cases}0, & x_9\le 3\\ x_9-3, & 3\le x_9\le 4\\ 5-x_9, & 4\le x_9\le 5\\ 0, & x_9\ge 5\end{cases}$
				Генерую "сильні" паролі, для зручності збереження користуюся менеджером паролів	H	$\mu_H(x_9)=\begin{cases}0, & x_9\le 4\\ x_9-4, & 4\le x_9\le 5\\ 1, & x_9\ge 5\end{cases}$
				Користуюся декількома такими, що запам'ятовуються, паролями для більшості акаунтів	M	$\mu_M(x_9)=\begin{cases}0, & x_9\le 2\\ x_9-2, & 2\le x_9\le 3\\ 4-x_9, & 3\le x_9\le 4\\ 0, & x_9\ge 4\end{cases}$
				Не запам'ятовую паролі, довіряю цю справу вбудованому в браузер сервісу автозбереження	ML	$\mu_{ML}(x_9)=\begin{cases}0, & x_9\le 1\\ x_9-1, & 1\le x_9\le 2\\ 3-x_9, & 2\le x_9\le 3\\ 0, & x_9\ge 3\end{cases}$
				Для зручності використовую один пароль для більшості облікових записів	L	$\mu_L(x_9)=\begin{cases}1, & x_9\le 1\\ 2-x_9, & 1\le x_9\le 2\\ 0, & x_9\ge 2\end{cases}$

ДОДАТОК В

Таблиця В.1 – Система нечіткого логічного виводу оцінки рівня КІБ організації

Змінна	Назва лінгвістичної змінної	Терм-множина	Тип ФН
1	2	3	4
ISC	Рівень КІБ організації	Початковий / фрагментарний / системний / керований / управління КІБ	gaussmf
y_1	Рівень ІБ-компетенції працівників	Високий / належний / задовільний, потребує підвищення / незадовільний, потребує навчання	gaussmf
x_{11}	Кваліфікація співробітників	Відповідає посаді / не відповідає посаді	trimf
x_{12}	Наявність професійних ІБ-компетенцій та soft-компетенцій у мірі, що задовольняє вимоги згідно посади, що займає співробітник	Результати співставлення оцінки персональної КІБ співробітника з вимогами до КІБ за посадою (повністю задовольняє / задовольняє більшість вимог / не відповідає вимогам)	trimf
Recom-menda-tion	Визначення напрямів подальшого розвитку фахівця для побудови індивідуальної траєкторії	Потребує додаткового навчання / не потребує додаткового навчання / не відповідає посаді	gaussmf
y_2	Позиція адміністрації до КІБ та підтримка	Підтримка достатня, КІБ приділена належна увага / увага приділена КІБ у найбільш важливих процесах / КІБ ігнорується	gaussmf
x_{21}	ІБ-політика організації	Сильна / задовільна / слабка / початкова	gaussmf
x_{211}	Наявність документально зафіксованих процесів та положень у вигляді ІБ-політики організації	Всі ІБ-процеси задокументовані / частково задокументовані / на початковій стадії / відсутні	trimf
x_{212}	Актуальність ІБ-політики	Актуальна / потребує перегляду / застаріла	trimf
x_{213}	Обізнаність співробітників щодо ІБ-політики організації	ІБ-політика організації доведена до кожного працівника / ІБ-політика відома керівникам структурних підрозділів та деяким працівникам / ІБ-політика відома керівникам структурних підрозділів / ІБ-політика не доведена до відповідальних	trimf
x_{214}	ІБ-політика організації доступна для стейкхолдерів через визначений порядок	ІБ-політика доступна за встановленим порядком / порядок не визначений / ІБ-політика не сформована	trimf

Продовження Таблиці В.1

1	2	3	4
x_{22}	Лідерство	Сильне / задовільне / слабке / початкове	Gaussmf
x_{221}	Узгодженість ІБ-політики з метою та стратегією розвитку організації	Співпадають / частково співпадають / не співпадають	trimf
x_{222}	Гарантії інтеграції СМІБ в процеси організації	Впроваджено / частково впроваджено / не впроваджено	trimf
x_{223}	Поінформованість щодо управління ІБ та відповідності вимогам СМІБ	Керівництво має актуальну інформацію / СМІБ не відповідає вимогам / інформація відсутня	trimf
x_{224}	Підтримка зусиль співробітників, спрямованих на розвиток СЗІБ	Постійна підтримка / частково здійснюється / не проводиться	trimf
x_{225}	Стимулювання безперервного вдосконалення СЗІБ	Постійна підтримка / частково здійснюється / не проводиться	trimf
x_{226}	Заохочення проявів лідерства на різних рівнях управління в межах встановленої відповідальності	Реалізується згідно положень / існують положення / положення відсутні	trimf
x_{23}	Використання провідного досвіду	Новітні наробітки / найкращі практики / власний досвід / не використовують	trimf
x_{24}	Інтеграція ІБ до внутрішніх процесів, що визначені організацією як важливі	Інтегровано до кожного важливого процесу / інтегровано до де-яких важливих процесів / процеси класифіковані, проте ІБ не включена / процеси не класифіковані	trimf
x_{25}	Врахування ІБ-аспектів при договірній діяльності	ІБ-аспекти включені до договорів (з врахуванням предмету договору) / ІБ не враховується про договірній діяльності	trimf
y_3	Контроль над діями, що пов’язані з ІБ	Сильний / достатній / слабкий / відсутній	gaussmf
x_{31}	Визначення меж та застосовність СМІБ для визначення областей впливу	Встановлено та задокументовано / встановлено / не встановлено	trimf
x_{32}	Актуальність СЗІБ	Підтримується на актуальному рівні / підтримується на достатньому рівні / неактуальна	gaussmf

Продовження Таблиці В.1

1	2	3	4
x_{321}	Безперервне вдосконалення СЗІБ за результатами аудитів ІБ-ризиків	СЗІБ впроваджена та підтримується постійно / СЗІБ впроваджена та підтримується / СЗІБ впроваджена, але не підтримується / СЗІБ не впроваджена	Trimf
x_{322}	Оцінка результативності внесених змін до СЗІБ	Проводиться / не проводиться	trimf
x_{33}	Встановлення вимірюваних (за можливості) цілей щодо ІБ організації	Визначені цілі для повномасштабного впровадження ІБ / встановлені цілі щодо деяких напрямів діяльності / цілі не встановлено	trimf
x_{34}	Планування	Відсутнє / слабке / реактивне / проактивне	gaussmf
x_{341}	Планування та проведення аудиту ІБ-ризиків	Проводяться згідно запланованого графіку / проводяться після ІБ-інциденту / не проводяться	trimf
x_{342}	Безперервність дій, спрямованих на обробку ІБ-ризиків	На постійній основі / періодичні / реакційні / не проводяться	trimf
x_{35}	Відповідність цілей актуальним вимогам до ІБ через оновлення	Надмірні / актуальні / неактуальні	trimf
x_{36}	Аудит СЗІБ з врахуванням попередніх результатів	Проводиться / проводиться разово / не проводиться	trimf
y_4	Комунікації	Відсутні / Початкові / зміцнені (установлені) / провідні	gaussmf
x_{41}	Зв’язки зі спеціалізованими спільнотами та галузевими кіберцентрами (ДССЗЗІ, кіберполіція, CERT-UA)	Встановлені контакти із державними службами / контакти із неформальними спільнотами / встановлені контакти із міжнародними службами та спільнотами / контакти відсутні	tramf
x_{42}	Обмін досвідом (через навчання, семінари, вебінари, тренінги, круглі столи, тематичні лекції (що їх читають провідні спеціалісти в ІБ-галузі), школи, акції, спрямовані на підвищення обізнаності користувачів) тощо	Регулярні заходи / реактивні заходи після інциденту / заходи відсутні	trimf
y_5	Емоційний клімат	Стабільно позитивний / позитивний / нейтральний / негативний / стабільно негативний	gaussmf

Завершення Таблиці В.1

1	2	3	4
x_{51}	Конвергенція місії, стратегічного плану розвитку, цінностей організації з цінностями та індивідуальними траєкторіями співробітників	Співпадають повністю / співпадають у більшості спостережуваних випадків / частково співпадають / не співпадають	trimf
x_{52}	Розуміння цілей, потреб та вимог партнерів та підрядників	Повністю співпадає / частково співпадає / не потребує / не визначено	trimf

ДОДАТОК Г

Таблиця Г.1 – Рекомендації щодо підвищення рівня КІБ (чатбот)

Номер питання	**Варіант відповіді (у вигляді терма)**			
	L	**LM**	**M**	**MH**
1	2	3	4	5
1	Використання тих самих гаджетів та акаунтів для робочої та особистої інформації порушує її цілісність та конфіденційність та може призвести до витоку з Вашої провини.	-	Зверніть увагу на доцільність використання окремих гаджетів та акаунтів для збереження конфіденційності інформації.	-
2	Пам’ятайте, що безпечне користування онлайн-банкінгом можливе лише за умов існування належного антивірусного захисту ПК/гаджета, сильної парольної політики, високої стійкості до методів соціальної інженерії.	-	Рідко користуючись онлайн-банкінгом, не слід забувати, що втрата цифрового ключа, мобільного телефону, на якому збережений пароль, або запам’ятовування пароля браузером призводить до фінансових збитків через злам.	-
3	Наявність блокувальника суттєво зменшує ризик несанкціонованого доступу до Вашої особистої або робочої інформації з боку третьої особи.	-	Використання блокувальника зменшує ризик витоку інформації, але подбайте про його надійність та складність.	-

1	2	3	4	5
4	Робота в ОС з правами адміністратора дає можливість вносити зміни в конфігураційні системні файли. Активність подібних прав доступу несе небезпеку вчинення несанкціонованих і прихованих змін в системні файли від імені адміністратора. Працюйте з правами Користувача!	-	Робота в ОС з правами адміністратора дає можливість вносити зміни в конфігураційні системні файли. Активність подібних прав доступу несе небезпеку вчинення несанкціонованих і прихованих змін в системні файли від імені адміністратора. Працюйте з правами Користувача!	-
5	Оновлення здійснює поліпшення захисту, закриваючи різні "дірки" в операційній системі та ПЗ, які можуть стати шляхом для проникнення шкідливих програм. І якщо у Вас недостатньо потужний антивірус, або його немає взагалі, і ви не оновлюєте систему, то вірогідність, що на ПК проникне вірус, майже стовідсоткова.	-	Деякі оновлення системи дозволяють бути більш захищеним від різних програм-шпигунів, про які Ви навіть не здогадуєтесь. Вибірково оновлюючи ОС, Ви ризикуєте збільшити свою вразливість або пропустити важливе оновлення.	-
6	Використання системами антивірусного ПЗ гарантує 99,99%	-	Для ефективного захисту рекомендовано встановлювати	-

1	2	3	4	5
	захищеність від шкідливого коду, або несанкціонованого доступу. Тому їх наявність вкрай важлива для ІБ.		антивірусне ПЗ на усіх обчислювальних пристроях для роботи з особистою та робочою інформацією.	
7	Використання антивірусних ПЗ є основою інформаційної захищеності гаджетів. Контролюйте їх наявність!	-	Зверніть увагу, що частота сканування суттєво впливає на показник захищеності інформації, виявляючи можливі загрози в процесі.	-
8	Варто звернути увагу на доречність поширення будь-якої інформації у соціальних мережах, так як можна розповсюдити або втратити персональну інформацію, та стати легкою жертвою для соціальних інженерів. Вкрай важливо пам’ятати, що навіть видалена зі сторінки інформація все одно зберігається на сервері. Уважно ставтеся до того, що викладаєте у СМ	-	Пам’ятайте, що важлива інформація з Вашої сторінки може стати джерелом для створення фейкового акаунту в іншій популярній соцмережі на допомогу соціальним інженерам.	Застарілі та малоактивні акаунти часто залишаються джерелом прихованих загроз. Вони все ще містять де-які особисті відомості про власника, а також соціальні зв’язки (друзі, колеги та ін.), не кажучи про втрату контролу над персональною сторінкою. Ці дані можуть стати у нагоді зловмисникам, тому видаляйте акаунти у разі невикористання!
9	Використання одного паролю збільшує вдалу	Рекомендовано звернути увагу на можливість	Використання одного або декількох	Якщо Вам не зручно запам'ятовувати

1	2	3	4	5
	вірогідність підбору пароля перебором або шляхом підбору за словником на підставі особистих даних або інформації з соціальних мереж.	використання менеджеру паролів, адже автозбереження у браузері може сприяти спрощеному доступу сторонньої особи до такої вразливої інформації, як облікові записи та паролі.	простих паролів призводить до швидкого витоку інформації з декількох систем або ресурсів одночасно лише з використанням додатку для підбору паролів. Завжди використовуйте окремі паролі для критично важливих облікових записів.	Ваші паролі, обачно обирайте місце їх зберігання. Доступ до Ваших паролів має бути тільки у вас!
10	Використання особової пошти на робочому місці може призвести до витоку робочої або особистої інформації, що призводить до втрати конфіденційності.	-	Використання особової пошти на робочому місці може призвести до витоку робочої або особистої інформації, що призводить до втрати конфіденційності.	-
11	Пам’ятайте, що важливо розділяти робочу та особисту інформацію за-для збереження її цілісності та конфіденційності, та зменшення ризику її втрати.	-	-	-
12	Наявність неліцензованого ПЗ збільшує вірогідність витоку інформації, так як не має необхідних мір захисту, та може містити у собі загрози, закладені	-	Рекомендовано оновлювати ПЗ, так як ліцензія дає право на фірмовий сервіс: отримання патчів, підтримку, додаткові можливості, а також гарантує,	-

1	2	3	4	5
	ще до початку використання.		що надана компанією копія продукту ідентична їх продукту.	

ДОДАТОК Д

АКТИ ВПРОВАДЖЕННЯ ТА ДОВІДКИ

ЧЕЗАРА CHEZARA

ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО
«ЧЕРНІГІВСЬКИЙ ЗАВОД РАДІОПРИЛАДІВ»
ПрАТ «ЧЕЗАРА»

вул. Захисників України, 25, м. Чернігів, 14030, Україна
E-mail: mail@chezara.com
www.chezara.com
тел.: +38 (04622) 3-43-44, 3-06-97
р/р 260080012021 в ПАТ «ПОЛІКОМБАНК»
МФО 353100

PRIVATE JOINT STOCK COMPANY
«CHERNIHIVSKYI ZAVOD RADIOPRYLADIV»
PrJSC «CHEZARA»

25, Zakhysnykiv Ukrainy Str., Chernihiv, 14030, Ukraine
E-mail: mail@chezara.com
www.chezara.com
tel./fax: +38 (04622) 3-43-44, 3-06-97
Account No. 260080012021 with the JSC «Policombank»
MFO 353100

код 14307392
Індивідуальний податковий номер 143073925261

№ 06/82 від "21" квітня 2021 р.

На № _____ від "___" _____ 20__ р.

«ЗАТВЕРДЖУЮ»
Генеральний директор ПрАТ «ЧЕЗАРА»
_____ **А. СВИРИДЕНКО**

АКТ ВПРОВАДЖЕННЯ

наукових результатів дисертаційної роботи ВОЙЦЕХОВСЬКОЇ Марії Михайлівни на тему «Інформаційна технологія оцінювання рівня культури інформаційної безпеки організації», представленої на здобуття вченого ступеня доктора філософії зі спеціальності 122 – «Комп'ютерні науки»

Комісія у складі: голови комісії – заступника генерального директора ПрАТ «ЧЕЗАРА», директора технічного ПАСІЧНОГО Миколи Михайловича, членів комісії: головного конструктора АНДРІЙЧЕНКА Владислава Миколайовича, заступника головного конструктора ІВАНОВА Володимира Євгеновича, начальника управління безпеки та режиму ПрАТ «ЧЕЗАРА» ТАРАСЮКА Анатолія Олександровича

за результатами вивчення наукових здобутків ВОЙЦЕХОВСЬКОЇ М.М., представлених протягом 2017-2020 рр. щодо запропонованої інформаційної технології оцінювання рівня культури інформаційної безпеки організації склала цей акт впровадження у практичну діяльність запропонованих рекомендацій. Запропонована технологія оцінки культури інформаційної безпеки персоналу в частині інформаційної безпеки підприємства дозволили:

1. Установити рівень захищеності підприємства та визначити слабкі місця у формуванні культури інформаційної безпеки персоналу.

2. Запровадити тестування персоналу на стадії підбору та приймання на роботу, на предмет виявлення базового рівня персональної культури інформаційної безпеки.
3. Розробити заходи щодо посилення інформаційного захисту структурних підрозділів підприємства за рахунок підвищення культури інформаційної безпеки персоналу.

Впровадження дисертаційних досліджень Войцеховської Марії Михайлівни сприяє підвищенню інформаційної безпеки організації, дозволяє попереджати виток конфіденційної інформації через необізнаність та недостатню культуру інформаційної безпеки персоналу, забезпечує доцільне формування кадрової політики в організації.

Голова комісії **Микола ПАСІЧНИЙ**

Члени комісії **В'ячеслав АНДРІЙЧЕНКО**

Володимир ІВАНОВ

Анатолій ТАРАСЮК

ДЕРЖАВНИЙ НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ВИПРОБУВАНЬ І СЕРТИФІКАЦІЇ ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ

МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
ДЕРЖАВНИЙ НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ВИПРОБУВАНЬ І СЕРТИФІКАЦІЇ ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ
Стрілецька, 1, Чернігів, 14033
dnvc@master.dod.ua
Код ЄДРПОУ 26614573
"26" 06 2020 року
№ 70/3/1938

Проректору з наукової роботи
Чернігівського національного
технологічного університету
Вікторії Маргасової
14013, м. Чернігів, вул. Шевченко, 95

ДОВІДКА ПРО ВПРОВАДЖЕННЯ
наукових результатів дисертаційної роботи
ВОЙЦЕХОВСЬКОЇ Марії Михайлівни на тему: "Інформаційна технологія оцінювання рівня культури інформаційної безпеки організації",
представленої на здобуття ступеня доктора філософії
зі спеціальності 122 – "Комп'ютерні науки"

Запропонована в дисертаційної роботі ВОЙЦЕХОВСЬКОЇ Марії Михайлівни на тему "Інформаційна технологія оцінювання рівня культури інформаційної безпеки організації" технологія оцінки культури інформаційної безпеки персоналу в частині інформаційної безпеки підприємства дозволили в Державному науково-дослідному інституті випробувань і сертифікації озброєння та військової техніки:

- запровадити тестування співробітників та визначити необхідність додаткового навчання при наданні доступу до інформаційних систем;
- визначити заходи з підвищення обізнаності кадрового складу з питань інформаційної безпеки.

Надані в дисертаційної роботі рекомендації стосовно наведених заходів впроваджені у процес забезпечення функціонування інформаційних систем інституту "Інформаційна система з доступом до мережі Internet" (ІСД-Internet) та "Система електронного документообігу" (СЕДО).

Заступник начальника Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки з наукової роботи
Лауреат Державної премії в галузі науки і техніки
кандидат технічних наук, старший науковий співробітник
Володимир ДМИТРІЄВ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЧЕРНІГІВСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

вул. Шевченка, 95, Чернігів, 14035, Україна

тел. +38(0462) 665-103;
факс +38(0462) 665-105
E-mail: cstu@stu.cn.ua
www.stu.cn.ua
Код ЄДРПОУ 05460798

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

CHERNIHIV NATIONAL UNIVERSITY OF TECHNOLOGY

95, Shevchenko str., Chernihiv, 14035, Ukraine

02.03.2020р. № 02-38/590

На № _____

Довідка

Видана аспірантці кафедри інформаційних технологій та програмної інженерії Войцеховській М.М. в тому, що результати дисертації впроваджені в навчальному процесі Чернігівського національного технологічного університету у такому вигляді:

1. В складі лабораторних робіт до курсу «Моделі і системи штучного інтелекту» для здобувачів вищої освіти за освітнім ступенем бакалавр спеціальності 121 – «Інженерія програмного забезпечення» освітньо-професійної програми «Інженерія програмного забезпечення», які містять рекомендації щодо використання ієрархічних нечітких логічних моделей на базі алгоритму Мамдані.
2. В ході впровадження результатів дисертації була виконана та захищена здобувачем вищої освіти 1 випускна кваліфікаційна робота, що містить використання нечіткої ієрархічної моделі для оцінки рівня персональної культури інформаційної безпеки за допомогою автоматизованої телефонної системи (чатботу).
3. У науковій роботі кафедри у проектах «Cyber Rapid Analysis for Defense Awareness of Real-time Situation – CyRADARS» за грантом NATO SPS, (grant agreement number: G5286)».

Проректор з наукової роботи В.Г. Маргасова