МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

СИДОРЕНКО Вікторія Миколаївна

УДК 004.056.5:656.7.08 (043.3)

МЕТОДИ ІДЕНТИФІКАЦІЇ ТА ОЦІНЮВАННЯ СТАНУ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ АВІАЦІЙНОЇ ГАЛУЗІ

21.05.01 – «Інформаційна безпека держави»

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ – 2018

Дисертацією є рукопис.

Робота виконана на кафедрі безпеки інформаційних технологій Національного авіаційного університету Міністерства освіти і науки України.

Науковий керівник: доктор технічних наук, доцент
Гнатюк Сергій Олександрович,
Національний авіаційний університет,
доцент кафедри безпеки інформаційних технологій.

Офіційні опоненти: доктор технічних наук, доцент
Казакова Надія Феліксівна,
Одеська державна академія технічного регулювання та якості, завідувач кафедри комп'ютерних та інформаційно-вимірювальних технологій;

кандидат технічних наук
Цуркан Василь Васильович,
Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «КПІ імені Ігоря Сікорського», доцент кафедри кібербезпеки та застосування автоматизованих інформаційних систем і технологій.

Захист відбудеться «29» травня 2018 р. о 15^{00} на засіданні спеціалізованої вченої ради Д 26.062.17 при Національному авіаційному університеті за адресою: 03058, м. Київ, пр. Космонавта Комарова, 1, ауд. 11.111.

З дисертацією можна ознайомитись у Науково-технічній бібліотеці Національного авіаційного університету за адресою: 03058, м. Київ, пр. Космонавта Комарова, 1.

Автореферат розісланий «27» квітня 2018 р.

В.о. ученого секретаря
спеціалізованої вченої ради
д.т.н., професор В. Козловський

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність. Сучасні тенденції розвитку інформаційно-комунікаційних технологій (ІКТ) спричинили феноменальну залежність суспільства від послуг, які надають різноманітні галузі інфраструктури. Сьогодні якість та доступність таких послуг є одними з головних показників розвитку інфраструктури держави, а забезпечення їх захисту та стабільного функціонування є найважливішою і обов'язковою складовою національної безпеки розвинених держав. Збільшення концентрації засобів та ресурсів для захисту електронних інфраструктур різних типів зумовило необхідність ранжування інфраструктурних об'єктів, виділення найважливіших з них та появи поняття критична інфраструктура (КІ) держави. Зазвичай, до цієї категорії відносять енергетичні та транспортні магістральні мережі, нафто- та газопроводи, морські порти, канали швидкісного та урядового зв'язку, системи життєзабезпечення мегаполісів, високо-технологічні підприємства та підприємства військово-промислового комплексу, а також центральні органи влади. Особливої уваги потребує авіаційна галузь, з огляду на необхідність забезпечення безперервної комунікації та взаємодії між наземними системами і повітряними суднами. Тому, першочерговим аспектом стає визначення об'єктів, які є критичними, оцінювання рівня їх важливості для забезпечення постійного функціонування, запобігання виникненню переривань роботи та збоїв в автоматизованих системах, що забезпечують їх роботу. Проте, необмежена кількість об'єктів і параметрів систем, які постійно варіюються, та важко прогнозована поведінка об'єктів з великою кількістю взаємозв'язків є основними причинами труднощів виявлення об'єктів КІ держави. Базовим компонентом КІ є інформаційна складова – критична інформаційна інфраструктура (КІІ). Основними причинами важливості КІІ є широке застосування ІКТ у всіх сферах людської діяльності, залежність від них громадян, суспільства і держави, а також збільшення уразливостей та потенційних загроз різного характеру (зокрема у кіберпросторі, т.з. кіберзагроз (КЗ)). Крім того, в деяких державах особливий акцент ставиться на значення КІ для нації, навіть саме визначення КІІ вживається як критична національна інформаційна інфраструктура. Що стосується України, то законодавча база регулювання захисту КІ знаходиться на початковій стадії формування, зокрема триває (поки що, на жаль, без особливих успіхів) процес ідентифікації об'єктів КІ держави у різних галузях.

Питаннями захисту КІІ держави займаються такі вітчизняні та закордонні вчені: Х. Алькарас, Д. Бірюков, Д. Бобро, Д. Грітсаліс, О. Довгань, Є. Єлісєєва, А. Кондратьєв, М. Мерабті, Л. Романо, Х. Сятерліс, І. Фовіно, В. Харченко та ін.

Проте переважна більшість досліджень не є системними: здебільшого вони орієнтовані на розробку й застосування превентивних та контрзаходів для захисту окремих об'єктів КІ чи КІІ; мало уваги приділяється механізмам формування переліку КІІ держави (ідентифікації, розрахунку критичності, оцінюванню КЗ та уразливостей), а також оцінюванню поточного стану кібербезпеки (КБ); для визначення рівня критичності використовуються відомі методи й методики (згідно міжнародних стандартів та рекомендованих практик), які не є формалізованими, що ускладнює їх застосування на загальнодержавному рівні, зокрема в авіаційній галузі.

З огляду на зазначене, розроблення методів ідентифікації та оцінювання стану кібербезпеки об'єктів критичної інформаційної інфраструктури авіаційної галузі є *актуальною науково-технічною задачею*, що має теоретичне і практичне значення.

Зв'язок роботи з науковими програмами, планами, темами. Тематика дисертаційної роботи та одержані результати безпосередньо пов'язані з «Основними науковими напрямами та найважливішими проблемами фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук НАН України на 2014-2018 роки», Постановою КМУ від 23 серпня 2016 року №563 «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави», зі Стратегією національної безпеки України від 26 травня 2015 року № 287/2015, зі Стратегією кібербезпеки України від 15 березня 2016 року №96/2016 і Рамковою програмою ЄС з досліджень та

інновацій «Горизонт 2020», зокрема за напрямком CIP-01-2016-2017 («Попередження, виявлення, реагування та мінімізація негативного впливу від фізичних та кіберзагроз на критичну інфраструктуру Європи»). Результати роботи відображені у звітах держбюджетних НДР НАУ «Квантово-криптографічні методи захисту критичної інформаційної інфраструктури держави» (д.р. № 0111U000171), НДР ІПМЕ ім. Г.Є. Пухова НАН України «Дослідження та розробка методів оцінювання захищеності інформації в розподілених високопродуктивних інформаційних системах при вирішенні задач енергетики», шифр «МОД-Д» (д.р. № 0114U002361), а також у звіті ДКР ДержНДІ Спецзв'язку, шифр «Інфраструктура» (д.р. № 0114U000038д), у яких здобувач брав участь у якості виконавця.

Мета і задачі дослідження. Метою дисертаційної роботи є забезпечення можливості ідентифікації та оцінювання стану кібербезпеки об'єктів критичної інформаційної інфраструктури авіаційної галузі.

Для досягнення поставленої мети необхідно розв'язати такі **основні задачі:**

– провести аналіз сучасних підходів до ідентифікації та оцінювання стану кібербезпеки об'єктів критичної інформаційної інфраструктури держави;

– розробити уніфіковану модель даних для формалізації процесу формування переліку об'єктів критичної інформаційної інфраструктури держави;

– розробити метод ідентифікації для визначення елементів інфраструктури галузі критичної інформаційної інфраструктури, їх взаємовпливу та впливу на функціональні операції системи;

– удосконалити метод визначення рівня важливості для кількісного і якісного оцінювання критичності об'єктів критичної інформаційної інфраструктури авіаційної галузі;

– розробити метод оцінювання рівня КБ для розрахунку кількісних параметрів, які характеризують захищеність об'єктів критичної інфраструктури в авіаційній галузі;

– створити спеціалізоване програмне забезпечення для верифікації розроблених у роботі моделі та методів.

Об'єктом дослідження є процеси ідентифікації та оцінювання стану КБ об'єктів КІІ.

Предметом дослідження є методи, моделі і засоби ідентифікації та оцінювання стану КБ об'єктів КІІ авіаційної галузі.

Методи дослідження. Проведені дослідження базуються на сучасних методах теорії захисту інформації (для визначення метрик у методі визначення рівня КБ), теорії множин (для формалізації етапів методу визначення рівня важливості критичних авіаційних інформаційних систем (КАІС)); системного та структурного аналізу (визначення відношень q-зв'язків КЗ та КАІС, ієрархічного представлення систем в уніфікованій моделі); теорії графів (для відображення елементів КІІ та їх функціональних процесів у методі ідентифікації об'єктів КІІ).

Наукова новизна одержаних результатів полягає у такому:

– *вперше розроблено* уніфіковану модель даних, яка за рахунок мультирівневої деталізації критичних авіаційних інформаційних систем, ієрархічного представлення множин, що характеризують системи та їх компоненти, а також введення матриці інцидентності кібербезпеки критичної інфраструктури, її симплексних комплексів та Q-аналізу, дозволяє формалізувати процес формування переліку об'єктів критичної інформаційної інфраструктури держави та визначити їх зв'язність (співвідношення q-зв'язків множин кіберзагроз та критичних авіаційних інформаційних систем);

– *вперше розроблено* метод ідентифікації, який за рахунок графоаналітичного відображення елементів критичної інфраструктури і їх функціональних процесів, формування можливих чинників і функцій впливу, а також матриці впливу елементів інфраструктури на функціональні операції, дає можливість визначити (ідентифікувати) елементи галузі критичної інформаційної інфраструктури, їх взаємовплив та вплив на функціональні операції критичної авіаційної інформаційної системи;

– *удосконалено* метод визначення рівня важливості, який за рахунок ієрархічного відображення множин, що характеризують критичні авіаційні інформаційні системи різних

рівнів деталізації, їх функції, порушення безперервності роботи, відповідні ознаки і наслідки, а також побудови тривимірної матриці критичності, причинно-наслідкової діаграми Ісікави і узгодження вагових коефіцієнтів критичності, дозволяє оцінювати критичність об'єктів критичної інформаційної інфраструктури авіаційної галузі та ранжувати їх для адекватного застосування коригувальних заходів;

– *отримав подальшого розвитку* метод оцінювання рівня кібербезпеки, який за рахунок представлення множин метрик кібербезпеки і метрик розвитку та впровадження інформаційно-комунікаційних технологій у вигляді зв'язаних списків, а також обчислення індексу кібербезпеки та відповідних метрик, дає можливість розрахувати кількісні параметри, які характеризують захищеність певної галузі чи критичної інформаційної інфраструктури держави в цілому.

Практичне значення одержаних результатів. Отримані в дисертаційній роботі результати можуть бути використані відповідними державними органами для формування переліку об'єктів КІІ з метою застосування адекватних механізмів захисту. Практична цінність роботи полягає у такому:

– створено методику, яка дозволяє формувати перелік об'єктів КІІ певної галузі та на загальнодержавному рівні;

– реалізовано програмний застосунок, який можна використовувати для ідентифікації елементів КІІ та визначення їх впливу на функціональні операції;

– створено методику визначення рівня важливості об'єктів КІІ, яка дає змогу кількісно оцінювати рівень важливості КАІС різних категорій та їх компонентів;

– результати дисертації впроваджені і використовуються у діяльності ТОВ «Акссонсофт», ДержНДІ Спецзв'язку, ІПМЕ ім. Г.Є. Пухова НАН України, а також у навчальному процесі кафедри безпеки інформаційних технологій НАУ для підвищення ефективності підготовки фахівців з КБ.

Особистий внесок здобувача. Основні положення і результати дисертаційної роботи, що виносяться до захисту, отримані автором самостійно. У роботах, написаних у співавторстві, автору належать: [1, 9] – розроблення формалізованої моделі даних для формування переліку об'єктів КІІ і визначення їх зв'язності; [2, 3, 11, 16, 26] – розроблення методу визначення рівня КБ галузі КІІ держави; [4, 7, 8, 24, 25] – теоретичне обґрунтування та експериментальне дослідження методу визначення рівня важливості об'єктів КІІ; [5, 12, 13, 18] – дефініційний аналіз щодо захисту КІІ держави; [6, 10, 14, 17, 21] – розроблення методу ідентифікації об'єктів КІІ в авіаційній галузі; [15, 19, 20, 22, 23] – аналіз методів оцінювання рівня критичності.

З робіт, що опубліковані у співавторстві, у дисертаційній роботі використовуються виключно результати, отримані особисто здобувачем.

Апробація результатів дисертації. Основні положення дисертаційної роботи доповідалися та обговорювалися на таких наукових конференціях: МНТК «ITSEC: Безпека інформаційних технологій» (Київ, 2016 р.), МНПК «Інтегровані інтелектуальні робототехнічні комплекси (ІІРТК)» (Київ, 2014 – 2016 рр.), ВНПК «Інноваційний потенціал світової науки — XXI сторіччя» (Запоріжжя, 2013 р.), НПК «Механізми управління безпекою підприємств в сучасних умовах господарювання» (Київ, 2013 р.), НПК «Актуальні проблеми управління інформаційною безпекою держави» (Київ, 2014 р.), Всесвітній конгрес «Авіація у XXI столітті» – «Безпека в авіації та космічні технології» (Київ, 2014 р.), ВНПК «Проблеми і перспективи розвитку авіації та космонавтики» (Київ, 2015 р.), НПК «Актуальні питання забезпечення кібербезпеки та захисту інформації» (Київ, 2016 – 2018 рр.), МНК «Украйна – България – Европейски Съюз: съвременно състояние и перспективи» (Варна, 2014 р.), Міжвідомчий міжрегіональний семінар Наукової ради НАН України «Технічні засоби захисту інформації» (Київ, 2017 р.) та ін.

Публікації. Основні положення дисертації опубліковано у 26 наукових працях, у тому числі: 1 розділ у колективній монографії, 10 наукових статей (3 – у закордонних рецензованих виданнях (1 з яких входить до до бази даних Scopus), 7 – у вітчизняних фахових наукових журналах), а також 15 матеріалів і тез доповідей на конференціях.

Структура роботи та її обсяг. Дисертація складається із анотації, вступу, чотирьох розділів, загальних висновків, додатків, списку використаних джерел і має 167 сторінок основного тексту, 54 рисунки, 49 таблиць, 16 сторінок додатків. Список використаних джерел містить 151 найменування і займає 16 сторінок. Загальний обсяг роботи 199 сторінок.

ОСНОВНА ЧАСТИНА

У **вступі** подано загальну характеристику роботи, обґрунтовано актуальність, сформульовано мету і задачі досліджень, відображено наукову новизну і практичну цінність отриманих результатів, наведено дані щодо їх апробації та впровадження.

У **першому розділі** проведено аналіз наукової літератури за темою дисертаційної роботи. Показано, що кожна структура має свої уразливості у вигляді критично важливих вузлів і об'єктів, посилань і платформ, незалежно від того, чи є вона комунікаційною, організаційною або будь-якою іншою мережею. Об'єднання критично важливих об'єктів в одну велику складну систему, порівняно нещодавно, дістало назву КІ. Активне вживання дефініції КІ почалось у другій половині 90-х років минулого сторіччя, здебільшого відносно розподілених великомасштабних інформаційно-телекомунікаційних систем (ІТС), центрів обробки даних, об'єднаних комунікаційних мереж тощо. Більшість розвинених держав самостійно робили спроби сформулювати визначення КІ, розробити підходи до її ідентифікації та державні стратегії захисту. Перелік життєво важливих КІ є різним для окремих держав і визначається відповідно до їх традицій, суспільних та політичних переконань, а також географічних та історичних особливостей кожної держави. Поява поняття КІІ пов'язане з необхідністю виділення центрального компонента КІ (інформаційної складової), вихід з ладу якої може нанести шкоду функціонуванню залежної КІ. Вперше концепція захисту КІІ була розроблена у США, а згодом – розвинута і адаптована у більшості розвинених держав світу. Аналіз вітчизняної нормативної бази свідчить, що галузь захисту КІІ в нашій державі перебуває на початковому етапі формування. Хоча чинним законодавством України й визначено окремі об'єкти соціально-економічної сфери, надзвичайні події на яких можуть призвести до суспільно небезпечних наслідків, проте вони не складають єдину систему. А спроби розробити єдиний перелік об'єктів КІІ в ІТС держави поки що не дали результатів. Крім того, відсутня чітко визначена понятійно-термінологічна основа у цій галузі, що, у свою чергу, значно ускладнює інтеграцію нашої держави до світового інформаційного простору. Встановлено, що для забезпечення ефективного захисту найбільш важливих об'єктів КІІ необхідно, перш за все, ідентифікувати ці об'єкти за певними критеріями (рис. 1).

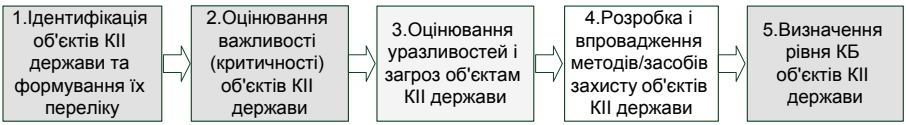


Рисунок 1 – Узагальнена схема етапів захисту КІІ держави

За результатами проведеного аналізу встановлено, що відомі підходи до ідентифікації об'єктів КІ орієнтовані, як правило, на економічні, екологічні, техногенні та інші системи безпеки держави і переважна їх більшість не враховує повної множини параметрів та особливостей КІІ (інформаційної складової). Найбільш ефективними є підходи, що базуються на теорії графів та імітаційному моделюванні. Крім того, за результатами аналізу було виділено низку методів оцінювання критичності ІТС як об'єктів КІІ держави – CORAS, HAZOP, FTA, OCTAVE, HACCP, FMECA. Встановлено, що вибір методів розрахунку критичності залежить від конкретних обставин: масштабу і складу ІТС, інформації, що обробляється у цій системі, складу і використовуваних засобів безпеки, наявності кваліфікованих експертів тощо. Також визначено, що найбільш універсальним серед проаналізованих методів є метод FMECA, у якому кожен вид відмови (порушення безперервної роботи) ранжується з урахуванням двох складових критичності – ймовірності та тяжкості наслідків відмови. Аналіз методів оцінювання

стану КБ дозволив, серед інших, виявити найбільш ефективний підхід для визначення рівня КБ (Global Cybersecurity Index) від ITU, який, окрім переваг, має низку недоліків, а саме: відсутність формалізованого опису, обгрунтування та чіткого кількісного визначення метрик КБ тощо. Таким чином, у першому розділі, на основі проведеного аналізу, визначено і обгрунтовано основні задачі дослідження, розв'язання яких необхідне для досягнення поставленої мети. На рис. 1 сірим кольором виділені етапи захисту КІІ держави, на забезпечення яких орієнтована дисертаційна робота.

Другий розділ присвячений формуванню переліку об'єктів КІІ держави шляхом розроблення уніфікованої моделі даних та методу ідентифікації об'єктів КІІ в авіаційній галузі. *Уніфікована модель даних* реалізується за допомогою наступної послідовності дій. Введення повної множини категорій систем КІІ у певній галузі $\mathbf{S} = \{\bigcup_{i=1}^{n} \mathbf{S}_i\} = \{\mathbf{S}_1, \mathbf{S}_2, \ldots, \mathbf{S}_n\}$, де $\mathbf{S}_i \subseteq \mathbf{S}$ $(i = \overline{1,n})$ – категорії систем у певній галузі КІ, n – загальна кількість категорій систем. Представлення множини категорій $\mathbf{S}_i$ у вигляді множини систем: $\mathbf{S}_i = \{\bigcup_{j=1}^{m_i} \mathbf{S}_{ij}\} = \{\mathbf{S}_{i1}, \mathbf{S}_{i2}, ..., \mathbf{S}_{im_i}\}$, де $\mathbf{S}_{ij} \subseteq \mathbf{S}_i$ $(i = \overline{1,n}$, $j = \overline{1,m_i})$ – системи i-ї категорії, m_i – кількість систем i-х категорій. Відображення множини систем $\mathbf{S}_{ij}$ за допомогою множини підсистем: $\mathbf{S}_{ij} = \{\bigcup_{k=1}^{r_{ij}} S_{ijk}\} = \{S_{ij1}, S_{ij2}, ..., S_{ijr_{ij}}\}$, де $S_{ijk} \subseteq \mathbf{S}_{ij}$ $(i = \overline{1,n}$, $j = \overline{1,m_i}$, $k = \overline{1,r_{ij}})$ – множина підсистем системи, r_{ij} – кількість підсистем ij-ї системи. Введення множини підсистем системи S_{ijk} у вигляді підмножини підсистем: $\mathbf{S}_{ijk} = \{\bigcup_{p=1}^{v_{ijk}} S_{ijkp}\} = \{S_{ijk1}, S_{ijk2}, ..., S_{ijkv_{ijk}}\}$, де $S_{ijkp} \subseteq \mathbf{S}_{ijk}$ $(i = \overline{1,n}$, $j = \overline{1,m_i}$, $k = \overline{1,r_{ij}}$, $p = \overline{1,v_{ijk}})$ – підмножина підсистем $\mathbf{S}_{ijk}$, v_{ijk} – кількість підмножин ijk-ї підсистеми. У залежності від можливостей деталізації категорій галузі КІІ підмножина підсистем S_{ijkp} може бути також представлена у вигляді підмножин з поглибленим рівнем деталізації. Тому повну множину категорій систем у галузі КІІ $\mathbf{S}$ необхідно представити у загальному вигляді таким чином: $\mathbf{S} = \{\bigcup_{i_1=1}^{n_0} \{\bigcup_{i_2=1}^{n_{i_1}} \{\ldots \{\bigcup_{i_l=1}^{n_{i_1,i_2,\ldots,i_{l-1}}} \mathbf{S}_{i_1,i_2,\ldots,i_l}\}\}\}\}$, де $\mathbf{S}_{i_1,i_2,\ldots,i_l} \subseteq \mathbf{S}$ $(i_1 = \overline{1,n_0}$, $i_2 = \overline{1,n_{i_1}}$, $i_l = \overline{1,n_{i_1,i_2,\ldots,i_{l-1}}})$ – рівні деталізації категорій систем $\mathbf{S}$, l – кількість рівнів деталізації категорій систем.

Для визначення зв'язності отриманих за допомогою уніфікованої моделі даних сформуємо матрицю інцидентності Δ (1), яка для визначеної множини КАІС ($\mathbf{Y} = \{\bigcup_{i=1}^{m} Y_i\} = \{Y_1, Y_2, \ldots, Y_m\}$, де $Y_i \subseteq \mathbf{Y}$ $(i = \overline{1,m})$, де m – загальна кількість систем) та множини КЗ об'єктам КІ держави ($\mathbf{X} = \{\bigcup_{j=1}^{n} X_i\} = \{X_1, X_2, \ldots, X_n\}$, де $X_i \subseteq \mathbf{X}$ $(j = \overline{1,n})$, де n – загальна кількість КЗ), відображає відношення впливу λ. Матриця інцидентності визначає відношення $\Delta = (\lambda_{ij})$, що характеризує можливість певної КЗ X_j вплинути на певну систему КАІС Y_i (де $\lambda_{ij} = 1$, якщо $(Y_i, X_j) \in 1$, та $\lambda_{ij} = 0$, якщо $(Y_i, X_j) \notin 1$).

$$\Delta = (\lambda_{ij})_{\substack{(i=\overline{1,m}),\\(j=\overline{1,n}).}} \tag{1}$$

Після чого, можливо сформувати множини вершин комплексу, що характеризують перелік можливих КЗ для певної системи $K_Y(X;\lambda)$, та перелік систем, на які може вплинуть певна КЗ $K_X\left(Y;\lambda^{-1}\right)$. Проте, якщо необхідно розглянути комплекс у цілому, доцільно використати поняття ланцюга зв'язку, який відображає той факт, що два симплекси можуть і не мати спільної грані, але можуть бути зв'язані за допомогою послідовності проміжних симплексів. Оскільки симплекційний комплекс є множиною симплексів, з'єднаних між собою за допомогою спільних граней, то за характеристику зв'язку можна брати величину грані, спільної для двох симплексів. Отже, якщо множини **Y** та **X** мають m і n елементів відповідно, то (1) є матрицею розміром $m\times n$, яка складається з нулів та одиниць. Добуток $\Delta\Delta^T$ – це число, що стоїть на місці (i, j) та є скалярним добутком рядків i та j матриці (1). Воно дорівнює числу одиниць, що знаходяться на одних і тих самих місцях у рядках i та j матриці (1) і відповідає значенню $(q+1)$, де q – розмірність спільної гарні симплексів σ_p і σ_r, заданих рядками i та j. Таким чином, для знаходження q - спільних граней усіх пар Y-симплексів у $K_Y(X;\lambda)$ необхідно: скласти матрицю $\Delta\Delta^T$ розміром $m\times m$; оцінити $\Delta\Delta^T-\Omega$, де $\Omega=(\omega_{ij})$, а $\omega_{ij}=1$ для $i,j=\overline{1,m}$. Цілі числа на діагоналі є розмірностями симплексів Y, а Q-аналіз здійснюється перевіркою інших комбінацій стовпчиків та рядків. Аналіз для $K_X\left(Y;\lambda^{-1}\right)$ виконується за допомогою складення матриці $\Delta^T\Delta-\Omega'$, де Ω' – матриця розміром $n\times n$, що складається з одиниць. Цілі числа на діагоналі також є розмірностями симплексів X, а Q-аналіз здійснюється перевіркою інших комбінацій стовпчиків та рядків. Кількість різних q-зв'язних комбінацій комплексу K позначається через число Q_q, а їх упорядковані в порядку спадання значення є першим структурним вектором комплексу. За допомогою структурного вектору та згідно виразу $\phi(K)=2\left[\sum_{i=0}^{N}(\mathrm{i}+)Q_i\right]/(\mathrm{N}+1)(\mathrm{N}+2)$, можна отримати і порівняти міру складності зазначених комплексів.

Також, у цьому розділі розроблений *метод ідентифікації об'єктів КІІ в авіаційній галузі,* який реалізується для певної системи (рівень деталізації $l=2$) і стосується лише елементів інформаційної інфраструктури (ЕІІ), які повністю відображають структуру обраного рівня деталізації. Розглянемо більш детально етапи реалізації зазначеного методу.

Етап 1. Формування елементів КІІ

Крок 1.1. Формування можливих ЕІІ. Кожен експерт з множини **E** ($\mathbf{E}=\{\bigcup_{j=1}^{N}E_j\}=\{E_1,E_2,\ldots,E_N\}$, $E_j\subseteq\mathbf{E}$ $(j=\overline{1,N})$ – експерти у галузі КІІ, N – загальна кількість експертів), формує всі можливі ЕІІ $\mathbf{L}^j=\{\bigcup_{k=1}^{h}L_k^j\}=\left\{L_1^j,L_2^j,\ldots,L_h^j\right\}$, $L_k^j\subseteq\mathbf{L}^j$ $(k=\overline{1,h})$ – можливі ЕІІ сформовані j-м експертом, h – кількість ЕІІ системи S_i. Можливі ЕІІ L_k^j формуються у вигляді матриці $L=\left(L_k^j\right)_{\substack{(k=\overline{1,h})\\(j=\overline{1,N})}}$ і можуть доповнюватись пустим елементом ω_0 таким чином, щоб всі рядки L мали однакову довжину.

Крок 1.2. Виділення унікальних ЕІІ. З отриманих в матриці L можливих ЕІІ виділяється множина $\mathbf{F}=\{\bigcup_{ai=1}^{e}F_{ai}\}=\left\{F_1,F_2,\ldots,F_e\right\}$, де $F_{ai}\subseteq\mathbf{F}$ $(ai=\overline{1,e})$ – унікальні ЕІІ, e – кількість унікальних ЕІІ.

Крок 1.3. Узгодження ЕІІ. Визначаються співпадіння елементів F_{ai} у матриці L у вигляді множини **V** ($\mathbf{V}=\{\bigcup_{bi=1}^{d}V_{bi}\}=\{V_1,V_2,\ldots,V_d\}$, де $V_{bi}\subseteq\mathbf{V}$ $(bi=\overline{1,d})$ – співпадіння ЕІІ F_{ai} у матриці

L, d – кількість відповідних співпадінь) та узгоджуються згідно виразу: $V_{bi} > \frac{N}{2}$. Отримані значення V_{bi} та їх відповідні ЕІІ, пропонуються у якості узгодженої множини елементів КІІ: $\mathbf{a} = \{\bigcup_{m=1}^{b} a_m\} = \{a_1, a_2, \ldots, a_b\}$, де $a_m \subseteq \mathbf{a}$ $(m = \overline{1,b})$ – елементи КІІ, які повністю відображають структуру системи КІІ, b – загальна кількість елементів КІІ.

Крок 1.4. Формування графу відображення ідентифікованих елементів КІІ.

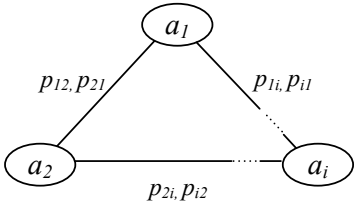


Рисунок 2 – Графоаналітичне відображення ідентифікованих a_m

Графоаналітичне відображення ідентифікованих елементів КІІ представлене неорієнтованим графом $\Gamma\left(\{a_m\}, \{p_{m\,m'}\}\right)$, де вершини a_m $(m = \overline{1,b})$ відповідають ідентифікованим елементам КІІ, а ребра $p_{m\,m'}$ ($m = \overline{1,b}$, $m' = \overline{1,b}$, $m \neq m'$) – зв'язкам між елементами a_m (рис. 2).

Етап 2. Формування можливих чинників впливу на елемент КІІ

Крок 2.1. Формування множини зон впливу. Вводиться множина $\mathbf{Z} = \{\bigcup_{ci=1}^{v} Z_{ci}\} = \{Z_1, Z_2, \ldots, Z_v\}$, де $Z_{ci} \subseteq \mathbf{Z}$ $(ci = \overline{1,v})$ – зони впливу на a_m, v – загальна кількість зон впливу.

Крок 2.2. Формування чинників впливу на елемент КІІ. Вводиться множина $\mathbf{\Phi} = \{\bigcup_{di=1}^{s} \Phi_{di}\} = \{\Phi_1, \Phi_2, \ldots, \Phi_s\}$, де $\Phi_{di} \subseteq \mathbf{\Phi}$ $(di = \overline{1,s})$ – чинники впливу на елемент КІІ, s – загальна кількість чинників впливу. Кожен Φ_{di} може бути представлений у вигляді набору $\Phi_{di}\left(Z_{ci}, O_{ei}^{\Phi_{di}}\right)$, де $\mathbf{O}^{\Phi_{di}} = \{\bigcup_{ei=1}^{z} O_{ei}^{\Phi_{di}}\} = \left\{O_1^{\Phi_{di}}, O_2^{\Phi_{di}}, \ldots, O_z^{\Phi_{di}}\right\}$, при чому $O_{ei}^{\Phi_{di}} \subseteq \mathbf{O}^{\Phi_{di}}$ $(ei = \overline{1,z})$ – параметри чинників впливу Φ_{di}, z – загальна кількість параметрів чинника Φ_{di}.

Етап 3. Визначення ступеню пошкодження та ваги впливу чинника на елемент КІІ. Для кожного визначеного Φ_{di} та елемента КІІ a_m, кожен експерт E_j фіксує значення двох величин $d_{gi}(a_m, \Phi_{di})$ та $\varphi_{gi}(a_m, \Phi_{di})$ (ступінь пошкодження елемента a_m та ваги впливу чинника Φ_{di} на елемент КІІ відповідно), де $gi = \overline{1,f}$, $f = b \cdot s$. Для оцінювання d_{gi} використовується лінгвістична шкала: *Damage absent* – «0» (вплив на a_m був незначний); *Middle damage* – «1» (вплив на a_m визвав значне пошкодження); *Complete failure* – «2» (вплив на a_m призвів до повного руйнування), а для φ_{gi} має виконуватись умова $\sum_{di=1}^{s} \varphi_{di}(a_m) = 1$. Далі відбувається узгодження отриманих оцінок d_{gi} та φ_{gi} за одним з відомих методів.

Етап 4. Формування функцій впливу елементів КІІ

Крок 4.1. Визначення відношень впливу між елементами КІІ. Для кожної можливої пари елементів КІІ $(a_m, a_{m'})$ (визначеної графом Γ, де $m = \overline{1,b}, m' = \overline{1,b}, m \neq m'$) кожен з експертів E_j

вказує значення відношення впливу r так $\left(r \in [-;+]\right)$: якщо пошкодження елементу a_m викликає пошкодження елементу $a_{m'}$, то ставиться «+», якщо ні – «–». Узгоджене значення впливу r_w для пари $(a_m, a_{m'})$ приймає значення «+», якщо кількість позитивних значень $K_{m\,m'} > \beta N$, де значення $0 < \beta < 1$ встановлюється заздалегідь та може переглядатися в залежності від системи КІІ.

Крок 4.2. Визначення функцій взаємовпливу між парами елементів КІІ. Парам елементів КІІ $(a_m, a_{m'})$, для яких на кроці 4.1 встановлено відношення впливу $r_w = $«+», необхідно вказати значення функції впливу $h_{m\,m'}(d_{gi})$, яке показує ступінь впливу на елемент $a_{m'}$, при пошкодженні елемента a_m (визначення $h_{m\,m'}$ проводиться відносно двох рівнів $d \in \{1,2\}$). Далі відбувається узгодження оцінок функції впливу $h^{y}_{m\,m'}(d)$ за одним з відомих методів.

Етап 5. Графоаналітичне відображення функціональних процесів системи КІІ

Відображення функціональних процесів системи КІІ можна представити орієнтованим ациклічним графом $G\left(\{B_{ii}\} \cup \{A_q\} \cup \{C_{ji}\}, \{P_{qq'}\}\right)$, де вершини A_q $(q = \overline{1,x})$ – функціональні операції,

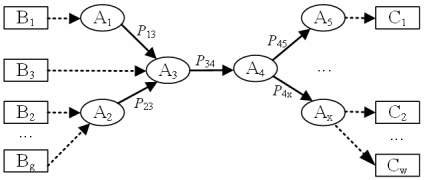


Рисунок 3 – Графоаналітичне відображення функціональних процесів системи КІІ

які виконує a_m, x – загальна кількість A_q, вершини B_{ii} $(ii = \overline{1,g})$, C_{ji} $(gi = \overline{1,w})$ – вхідні та вихідні дані A_q відповідно (g – загальна кількість вхідних даних, w – загальна кількість вихідних даних), а ребра $P_{qq'}$ – зв'язки між операціями $A_q, A_{q'}$, де $q = \overline{1,x}$, $q' = \overline{1,x}$, $q \neq q'$ (рис. 3).

Таке представлення дозволяє відобразити у зручному вигляді формалізований опис функціональних етапів операцій та зв'язків між ними, а також відповідні вхідні та вихідні дані.

Етап 6. Оцінювання якості функціонування системи КІ. Кожен експерт E_j формує матрицю якості виконання функціональних операцій $Q^q_d\left(d(a_m)\right)$, що відображає виконання операції A_q за умови, що елемент a_m має відповідне пошкодження $d(a_m)$, де верхній індекс виразу Q^q_d відповідає номеру операції, а нижній – значенню пошкодження $d \in \{0,1,2\}$. Для оцінювання значення Q^q_d вводиться лінгвістична шкала: *Normal* – «0» (операція виконується у відповідності з регламентом); *Deviation* – «1» (операція виконується, але спостерігаються суттєві відхилення від регламенту); *Interruption* – «2» (операція не виконується). Аналогічно до етапів 3-4, відбувається узгодження оцінок Q^q_d.

Ранжування узгоджених оцінок Q^q_d відбувається шляхом порівняння суми кількісних показників якості, одержаних від різних a_m, та визначається наступним чином: $\{VEI_1 > VEI_2 >, ..., > VEI_o\}$, де множина $\mathbf{VEI} = \{\bigcup_{li=1}^{o} VEI_{li}\} = \{VEI_1, VEI_2, ..., VEI_o\}$, у якій $VEI_{li} \subseteq \mathbf{VEI}$ $(li = \overline{1,o})$ – ранжовані за порядком важливості для системи елементи КІІ, o – номер за порядком ранжованих a_m відносно суми показників якості (до того ж, $o = b$).

Отже, розроблений метод ідентифікації об'єктів КІІ дає можливість ідентифікувати елементи галузі КІІ, визначати їх взаємовплив та вплив на функціональні операції КАІС.

У **третьому розділі** наведено розроблення методів визначення рівня важливості КІІ та рівня КБ галузі КІІ держави. Запропонований *метод визначення рівня важливості КІІ в авіаційній галузі* (схема його реалізації відображена на рис. 4) реалізується у такі 11 етапів:

Етап 1. Визначення компонентів систем та встановлення рівня деталізації

Крок 1.1. – 1.3. Використовуючи елементи теорії множин, вводяться множини класів $\mathbf{S}$, систем $\mathbf{S}_i$ та підсистем $\mathbf{S}_{ij}$ згідно розробленої уніфікованої моделі даних, при $l = 3$ (див. рис. 4).

Крок 1.4. Вводиться множина компонентів: $\mathbf{C} = \{\bigcup_{i=1}^{b} C_i\} = \{C_1, C_2, ..., C_b\}$, де $C_i \subseteq \mathbf{C}$ $(i = \overline{1,b})$ – компоненти, b – загальна кількість компонентів ij -ї системи.

Крок 1.5. Встановлюється мінімальний рівень деталізації системи: $Det_{\min} = C_i$.

Етап 2. Визначення функцій кожного виявленого компонента системи. Множина функцій $\mathbf{F}$ представляється у такому вигляді: $\mathbf{F} = \{\bigcup_{i=1}^{l} F_i\} = \{F_1, F_2, ..., F_l\}$, де $F_i \subseteq \mathbf{F}$ $(i = \overline{1,l'})$ – функції компонентів КАІС, l' – загальна кількість функцій.

Етап 3. Визначення переліку можливих переривань роботи кожного компонента системи. Вводиться множина можливих переривань роботи: $\mathbf{D} = \{\bigcup_{i=1}^{p} D_i\} = \{D_1, D_2, ..., D_p\}$, де $D_i \subseteq \mathbf{D}$ $(i = \overline{1,p})$ – переривання роботи компонента C_i, p – загальна кількість D_i.

Етап 4. Визначення наслідків кожного можливого переривання роботи. Для визначення наслідків кожного можливого D_i вводиться множина наслідків: $\mathbf{E} = \{\bigcup_{i=1}^{q} E_i\} = \{E_1, E_2, ..., E_q\}$, де $E_i \subseteq \mathbf{E}$ $(i = \overline{1,q})$ – наслідки D_i, q – загальна кількість наслідків D_i.

Етап 5. Ідентифікація ознак виявлення переривання роботи. Вводиться множина ознак: $\mathbf{O} = \{\bigcup_{i=1}^{r} O_i\} = \{O_1, O_2, ..., O_r\}$, де $O_i \subseteq \mathbf{O}$ $(i = \overline{1,r})$ – ознаки виявлення D_i, r – загальна кількість ознак. Для визначення O_i кожного можливого D_i вводиться функцію еквівалентності $E(O_i, D_i) = \begin{cases} 1, \textit{ при } O_i = D_i; \\ 0, \textit{ при } O_i \neq D_i, \end{cases}$ яка приймає значення «1» при виявленні ознаки D_i та «0» при не виявленні відповідної ознаки D_i.

Етап 6. Ідентифікація способів виявлення переривань роботи. Вводиться множина $\mathbf{W} = \{\bigcup_{i=1}^{s} W_i\} = \{W_1, W_2, ..., W_s\}$, де $W_i \subseteq \mathbf{W}$ $(i = \overline{1,s})$ – способи виявлення D_i, s – загальна кількість способів виявлення D_i.

Етап 7. Побудова тривимірної матриці критичності. Для побудови матриці критичності (див. рис. 4) необхідно для переривань D_i визначити: частоту (ймовірність) настання D_i, ступінь тяжкості наслідків D_i та їх кількість при фіксованій категорії тяжкості і частоті.

Етап 8. Розрахунок рангу критичності ймовірних переривань. Вводиться множина значень рангу критичності $\mathbf{R}$ наступним чином: $\mathbf{R} = \{\bigcup_{i=1}^{w} R_i\} = \{R_1, R_2, ..., R_w\}$, де $R_i \subseteq \mathbf{R}$ $(i = \overline{1,w})$ – ранги критичності D_i, w – загальна кількість показників рангів критичності.

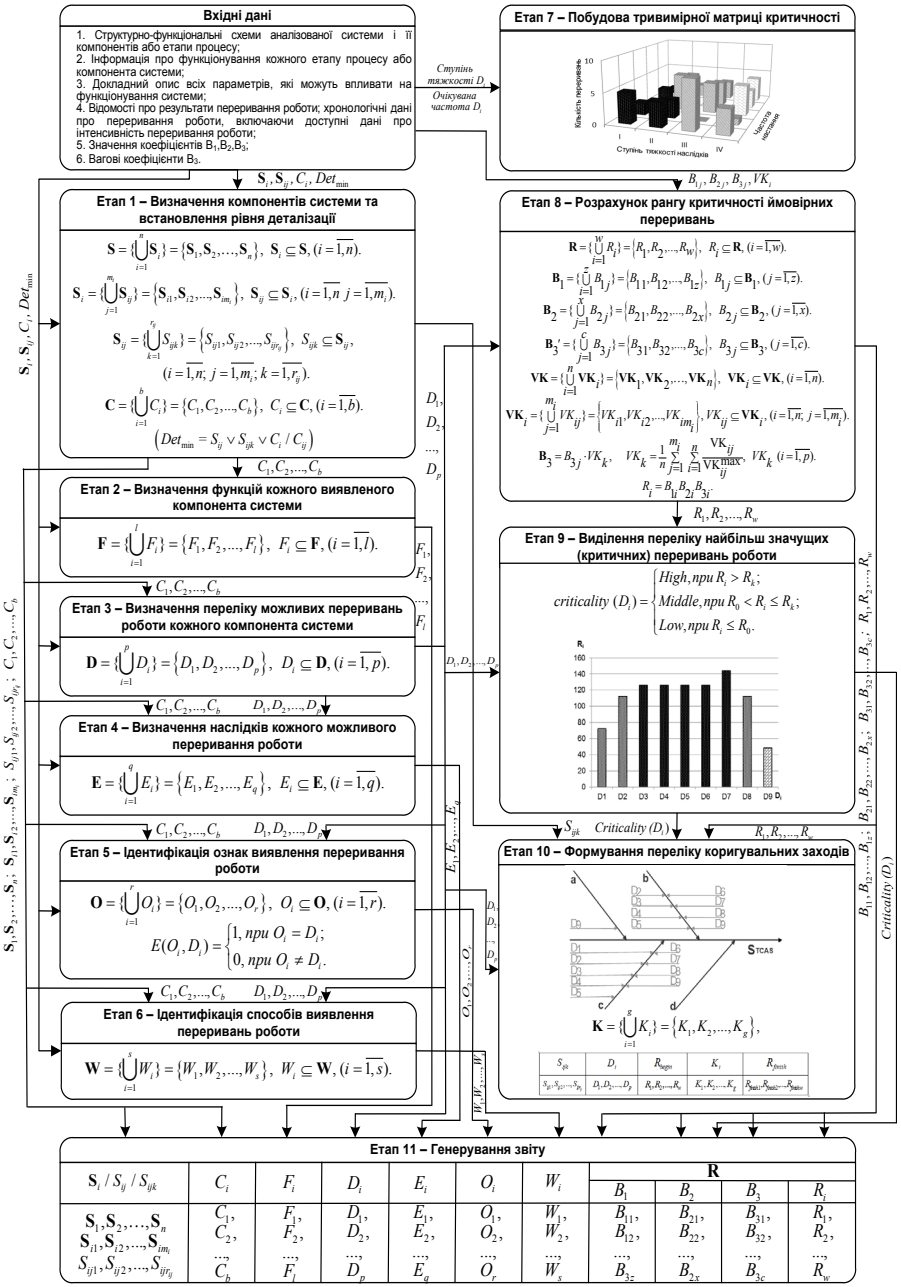


Рисунок 4 – Схема реалізації методу визначення рівня важливості об'єктів КІІ

Ранг критичності D_i розраховується згідно (2):

$$R_i = B_{1j} \cdot B_{2j} \cdot B_{3j}. \quad (2)$$

Крок 8.1. Для визначення показника B_{1j} (оцінка частоти настання потенційного D_i компонента C_i) вводиться відповідна множина: $\mathbf{B}_1 = \{\bigcup_{j=1}^{z} B_{1j}\} = \{B_{11}, B_{12}, ..., B_{1z}\}$, де $B_{1j} \subseteq \mathbf{B}_1$ $(j = \overline{1,z})$, значення z сформовані апріорі у залежності від типу КАІС.

Крок 8.2. Для визначення показника B_{2j} (оцінка ймовірності виявлення D_i компонента C_i до його проявлення) вводиться множина: $\mathbf{B}_2 = \{\bigcup_{j=1}^{x} B_{2j}\} = \{B_{21}, B_{22}, ..., B_{2x}\}$, де $B_{2j} \subseteq \mathbf{B}_2$ $(j = \overline{1,x})$, значення x аналогічно формуються апріорі в залежності від типу КАІС.

Крок 8.3. Аналогічним чином, для визначення показника B_{3j} (оцінка тяжкості D_i компонента C_i) вводиться множина: $\mathbf{B}_3 = \{\bigcup_{j=1}^{c} B_{3j}\} = \{B_{31}, B_{32}, ..., B_{3c}\}$, де значення c формуються аналогічно до значень z та x.

Коефіцієнт B_{3j} пов'язаний з тяжкістю наслідків D_i і появою загрози для безпеки людей, навколишнього середовища та має постійно велике значення, тому виникає необхідність розробки додаткових вагових коефіцієнтів.

Крок 8.4. Вводиться множина вагових коефіцієнтів: $\mathbf{VK} = \{\bigcup_{i=1}^{n} \mathbf{VK}_i\} = \{\mathbf{VK}_1, \mathbf{VK}_2, ..., \mathbf{VK}_n\}$, де $\mathbf{VK}_i \subseteq \mathbf{VK}$ $(i = \overline{1,n})$ – критерії вагових коефіцієнтів, n – загальна кількість критеріїв. Множина $\mathbf{VK}_i$ може бути представлена як: $\mathbf{VK}_i = \{\bigcup_{j=1}^{m_i} VK_{ij}\} = \{VK_{i1}, VK_{i2}, ..., VK_{im_i}\}$, де $VK_{ij} \subseteq \mathbf{VK}_i$ $(i = \overline{1,n},\ j = \overline{1,m_i})$ – коефіцієнти i-го критерію, m_i – кількість значень i-го критерію. Тоді елементи множини показників $\mathbf{B}_3'$ визначаються наступним чином: $B_3' = B_{3j} \cdot VK_k$, де значення вагового коефіцієнта VK_k $(k = \overline{1,p})$ для кожного можливого D_i розраховується таким чином: $VK_k = \frac{1}{\mathrm{n}} \sum_{j=1}^{m_i} \sum_{i=1}^{n} \frac{VK_{ij}}{VK_{ij}^{max}}$, де VK_{ij}^{max} – максимальне значення коефіцієнта i-го критерію.

Крок 8.5. Розраховується ранг критичності R_i кожного з перерахованих D_i згідно (2).

Етап 9. Виділення переліку критичних переривань роботи. Виділення критичних D_i здійснюється шляхом порівняння рангу R_i з деякими граничними його значеннями R_0 та R_k. Встановлено, що критичність змінюється в діапазоні $[R_{\min}; R_{\max}]$, де $R_{\min} = B_{11} \cdot B_{21} \cdot B_{31}$, $R_{\max} = B_{1z} \cdot B_{2x} \cdot B_{3c}$. Згідно міжнародних стандартів, граничне значення встановлюють так: $R_k = \frac{1}{2}(B_{1z} \cdot B_{2x} \cdot B_{3c})$, при чому $R_{\min} < R_k < R_{\max}$, де $R_{\min} = 1$, $R_{\max} = 10^3$, $R_k = 125$, а рекомендоване значення $R_0 = 60$. Далі вводяться правила для визначення критичності D_i –

$criticality\ (D_i) \in \{High, Middle, Low\}: criticality\ (D_i) = \begin{cases} High, npu\ R_i > R_k; \\ Middle, npu\ R_0 < R_i \le R_k; \\ Low, npu\ R_i \le R_0. \end{cases}$ Крім того, для ранжування критичних D_i використовується стовпчаста діаграма Парето (див. рис. 4), яка будується окремо для кожної S_{ij}, де за горизонтальною віссю діаграми відкладаються D_i, а за вертикальною – R_i.

Етап 10. Формування переліку коригувальних заходів. Для складання переліку коригувальних заходів відбувається виявлення причинно-наслідкових закономірностей за діаграмою Ісікави (див. рис. 4), яка для кожного R_i (рівнів *High* та *Middle*) системи S_{ij} відображає параметри (причини), з якими пов'язане виникнення D_i, а саме через помилки: користувачів (a), програмного забезпечення (b), апаратного забезпечення (c), мережевих технологій (d). Після чого, вводиться множина коригувальних заходів: $\mathbf{K} = \{\bigcup_{i=1}^{g} K_i\} = \{K_1, K_2, ..., K_g\}$, де $K_i \subseteq \mathbf{K}$ $(i = \overline{1,g})$ – коригувальні заходи, g – загальна кількість коригувальних заходів. Оцінювання ефективності K_i здійснюється шляхом повторного розрахунку R_i (див. етап 8). Далі, з огляду на початкові значення R_{begin} (до імплементації K_i) і кінцеві R_{finish} (після імплементації K_i): якщо $R_{finish} < R_k$ то K_i є спрямованими на підвищення КБ і їх можна рекомендувати до використання.

Етап 11. Генерування звіту. На цьому етапі відбувається систематизація даних, отриманих на етапах 1-10 ($\mathbf{S}_i, S_{ij}, C_i, F_i, D_i, E_i, O_i, W_i, R_i$), візуалізація якісних та обчислення кількісних параметрів, що характеризують критичність КАІС (див. рис. 4).

Таким чином, запропонований метод дозволяє оцінювати критичність об'єктів КІІ та ранжувати їх для адекватного застосування коригувальних заходів.

Крім того, у цьому розділі дисертації розроблено *метод оцінювання рівня КБ галузі КІІ держави,* який реалізується у такі 3 базові етапи:

Етап 1. Визначення метрик та індексу КБ галузі КІ

Крок 1.1. Формування множин метрик КБ. Вводиться базова множина метрик КБ: $\mathbf{P} = \{\bigcup_{i=1}^{n} \mathbf{P}_i\} = \{\mathbf{P}_1, \mathbf{P}_2, ..., \mathbf{P}_n\}$, де $\mathbf{P}_i \subseteq \mathbf{P}$ $(i = \overline{1,n})$ – підмножина наборів метрик, n – загальна кількість наборів. Множину $\mathbf{P}$ можна представити у вигляді зв'язаних списків, що відображено на рис. 5.

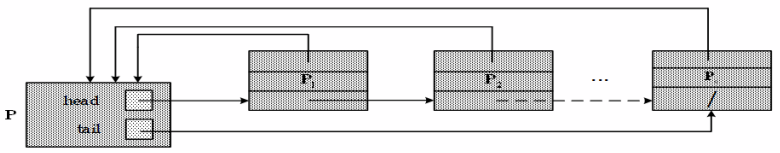


Рисунок 5 – Представлення множини $\mathbf{P}$ у вигляді зв'язаних списків

Множина $\mathbf{P}_i$ може бути представлена у вигляді ієрархічної системи підмножин: $\mathbf{P}_i = \{\bigcup_{j=1}^{m_i} P_{ij}\} = \{P_{i1}, P_{i2}, ..., P_{im_i}\}$, де P_{ij} $(i = \overline{1,n},\ j = \overline{1,m_i})$ – метрики i-го набору (діапазон значень метрик визначається згідно відповідних стандартів та рекомендованих практик у певній галузі КІІ з урахуванням її особливостей), m_i – кількість метрик i-го набору. Аналогічно, множину $\mathbf{P}_i$ можна представити у вигляді зв'язаних списків, що відображено на рис. 6.

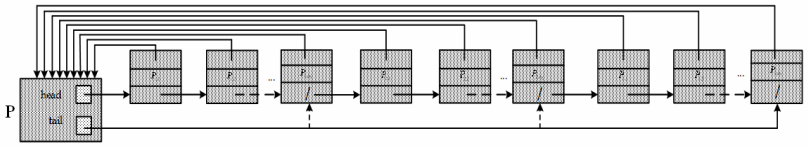


Рисунок 6 – Представлення множини $\mathbf{P}_i$ у вигляді зв'язаних списків

Крок 1.2. Обчислення індексу, що характеризує рівень КБ галузі КІІ. Обчислення індексу, що характеризує рівень КБ певної галузі КІІ відбувається, за допомогою (3), де $\sum_{P_{ij}}^{max}$ – максимально можлива сума значень метрик P_{ij}.

$$\mathbf{I}_{CS} = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m_i} P_{ij} \cdot 100\%}{\sum_{P_{ij}}^{max}}, \sum_{P_{ij}}^{max} \neq 0. \quad (3)$$

Етап 2. Визначення метрик розвитку та впровадження ІКТ у галузі КІІ

Крок 2.1. Формалізація метрик ІКТ. Вводиться множина метрик, які характеризують розвиток і впровадження ІКТ: $\mathbf{M} = \{\bigcup_{k=1}^{q} \mathbf{M}_k\} = \{\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_q\}$, де $\mathbf{M}_k \subseteq \mathbf{M}$ $(k = \overline{1,q})$ – підмножина метрик розвитку і впровадження ІКТ, q – кількість підмножин метрик. Множина $\mathbf{M}_k$ може бути представлена таким чином: $\mathbf{M}_k = \{\bigcup_{r=1}^{p_i} M_{kr}\} = \{M_{k1}, M_{k2}, \ldots, M_{kp_i}\}$, де M_{kr} $(k = \overline{1,q}, r = \overline{1,p_i})$ – метрики k-ї множини, p_i – кількість метрик k-ї множини.

Аналогічно до рис. 5-6, множини $\mathbf{M}$ та $\mathbf{M}_k$ можна представити у вигляді зв'язних списків.

Крок 2.2. Обчислення формалізованих метрик ІКТ. Метрики, що характеризують розвиток та впровадження ІКТ в певній галузі КІІ, обчислюються згідно (4). Слід зауважити, що так як метрики $\mathbf{M}_k$ можуть мати різні розмірності, на цьому кроці також відбувається їх нормування.

$$\mathbf{I}_{ICS} = \frac{\sum_{i=1}^{q} M_i \cdot 100\%}{q}, q \neq 0. \quad (4)$$

Етап 3. Розрахунок кількісних параметрів, які характеризують рівень КБ галузі КІІ. На основі (3) та (4) можемо отримати кількісні параметри (5), які характеризують рівень КБ.

$$\mathbf{I}_{ratio} = \mathbf{I}_{CS} - \mathbf{I}_{ICS} = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m_i} P_{ij} \cdot 100\%}{\sum_{P_{ij}}^{max}} - \frac{\sum_{k=1}^{q} \mathbf{M}_k}{q}, \sum_{P_{ij}}^{max} \neq 0, q \neq 0. \quad (5)$$

Таким чином, зазначений метод дає можливість розрахувати кількісні параметри, які характеризують захищеність певної галузі КІ, регіону, держави тощо.

Четвертий розділ присвячено практичним реалізаціям та експериментальним дослідженням розроблених методів. Розроблено методику проведення експериментального дослідження, обґрунтовано доцільність вибору бази експериментів, визначено мету та задачі експериментів, вхідні та вихідні параметри, гіпотезу і критерії дослідження, достатність експериментальних об'єктів та послідовність необхідних дій.

На основі запропонованої у другому розділі дисертації уніфікованої моделі даних було розроблено методику, за допомогою якої сформовано перелік об'єктів КІІ для авіаційної галузі, у

результаті чого, при рівні деталізації $l = 4$, виділено 3 множини категорій, 17 множин систем, 97 множин підсистем, 125 підсистем КАІС. Фрагмент сформованого переліку наведено у табл. 1.

Таблиця 1

Сформований перелік об'єктів КІІ в авіаційній галузі

Рівні деталізації	Параметри	Системи / підсистеми КАІС
$l = 1$	$n = 3$	**ISAO, BSPS, ISAA**
$l = 2$	$m_1 = 5, m_2 = 7, m_3 = 5.$	**SAE, RZZP, SSP, SOD, SMZ, SPS, SZV, NAVS, SSPZ, OSL, SVI, ABSK, CRS, GDS, IDS, BSP, DCS**
$l = 3$	$r_{1.1} = 5, r_{1.2} = 4, ..., r_{3.5} = 5.$	**SAPE, SANE**, *..., HCS*
$l = 4$	$v_{1.1.1} = 3, v_{1.1.2} = 6, ..., v_{3.5.2} = 3.$	*NRPZ, CPDLC, ..., TTSH*

Отриманий перелік множин S_{ij} (рівень деталізації $l = 2$) був використаний для визначення зв'язності множин КАІС та КЗ. На основі (1) була побудована матриця інцидентності $\Delta_{KAIS\_THREATS}$ (рис. 7), при $i = \overline{1,17}$, $j = \overline{1,19}$, що відображає бінарний зв'язок множин та характеризує можливість певної КЗ X_j вплинути на певну КАІС Y_i.

	X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9	X_{10}	X_{11}	X_{12}	X_{13}	X_{14}	X_{15}	X_{16}	X_{17}	X_{18}	X_{19}
Y_1	1	1	1	0	1	1	0	1	1	1	0	1	0	0	1	1	1	1	0
Y_2	1	0	1	0	1	1	0	1	1	1	0	0	0	0	1	1	1	1	0
Y_3	1	0	0	0	1	1	0	1	1	1	1	1	1	0	1	1	0	1	0
Y_4	1	0	0	0	1	1	0	1	1	1	1	1	1	0	0	1	1	0	1	0
Y_5	1	1	0	1	1	0	0	1	1	1	1	1	1	0	0	1	0	0	0
Y_6	1	0	1	0	1	0	0	1	1	1	1	1	1	0	1	1	0	0	0
Y_7	1	0	1	1	1	1	0	1	1	1	1	1	1	0	0	1	1	1	1
Y_8	1	0	1	0	1	1	0	1	1	1	1	1	1	0	0	1	1	1	0
Y_9	1	0	1	0	1	1	1	1	1	1	0	1	1	0	1	1	1	1	0
Y_{10}	1	0	0	0	1	1	0	1	0	1	0	0	0	0	0	1	0	0	0
Y_{11}	1	1	1	0	1	1	0	1	1	1	0	0	0	0	1	0	1	1	0
Y_{12}	1	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	0	0
Y_{13}	1	0	1	0	1	1	0	1	0	0	0	1	0	1	1	1	1	1	1
Y_{14}	1	0	1	0	1	1	0	1	0	0	0	0	0	1	1	1	0	1	1
Y_{15}	1	0	1	0	1	1	0	1	0	0	0	0	0	1	1	1	0	1	0
Y_{16}	1	0	1	0	1	1	0	0	0	0	0	0	0	1	1	1	0	1	0
Y_{17}	1	1	1	1	1	1	0	1	1	0	0	1	1	1	1	1	1	1	1

Рисунок 7 – Матриця інцидентності $\Delta_{KAIS\_THREATS}$

Після чого був проведений Q-аналіз зв'язків цих множин (рис. 8), який показав, що відношення q-зв'язків множин КЗ має більш високу зв'язність у порівнянні з аналогічним відношеннями q-зв'язних множин КАІС (зокрема $Q_Y = \{1,1,1,2,2,5,1,1,1,1,1\}$, $Q_X = \{1,1,1,2,2,1,1,1,1,1,3,1,1,1\}$), а це свідчить, що реалізація однієї КЗ може ініціювати каскадний ефект на інші зв'язані КЗ та призвести до важких, а іноді і руйнівних наслідків для певної КАІС. Крім того, відповідно до отриманих структурних векторів Q_Y, Q_X, була обчислена міра складності комплексів: $\phi_{KAIS} = 1{,}39$ та $\phi_{THREATS} = 1{,}13$, що свідчить про більшу «складність» КАІС.

Y_1	Y_2	Y_3	Y_4	Y_5	Y_6	Y_7	Y_8	Y_9	Y_{10}	Y_{11}	Y_{12}	Y_{13}	Y_{14}	Y_{15}	Y_{16}	Y_{17}	
12	10	9	9	7	8	11	11	11	5	10	5	9	7	7	6	11	Y_1
	10	8	8	5	7	10	10	10	5	9	4	8	7	7	6	9	Y_2
		11	10	8	9	10	10	10	5	7	3	7	6	6	5	9	Y_3
			10	7	8	10	10	9	5	7	3	7	6	6	5	8	Y_4
				10	8	8	7	7	4	5	4	4	3	3	2	8	Y_5
					10	9	9	9	4	6	4	6	5	5	4	8	Y_6
						14	12	11	5	9	4	10	8	7	6	12	Y_7
							12	11	5	9	4	9	7	7	6	10	Y_8
								13	5	9	5	9	7	7	6	11	Y_9
									5	4	2	4	4	4	3	4	Y_{10}
										10	5	7	6	6	5	9	Y_{11}
											6	3	3	3	2	5	Y_{12}
												11	9	8	7	11	Y_{13}
													9	8	7	9	Y_{14}
														8	7	8	Y_{15}
															7	7	Y_{16}
																15	Y_{17}

а)

X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9	X_{10}	X_{11}	X_{12}	X_{13}	X_{14}	X_{15}	X_{16}	X_{17}	X_{18}	X_{19}	
16	4	12	2	16	13	1	15	11	10	5	9	4	4	13	14	7	12	3	X_1
	4	3	1	4	2	0	4	4	2	0	2	1	0	2	2	2	2	0	X_2
		12	1	12	10	1	11	8	6	2	6	2	4	11	10	7	10	3	X_3
			2	2	1	0	2	2	1	1	2	1	0	1	2	1	1	1	X_4
				16	13	1	15	11	10	5	9	4	4	13	14	7	12	3	X_5
					13	0	12	8	8	3	7	2	4	12	12	7	12	3	X_6
						1	1	1	0	0	0	0	0	0	0	0	0	0	X_7
							15	11	10	5	9	4	3	12	13	7	11	3	X_8
								11	9	5	8	4	0	9	9	6	8	1	X_9
									10	5	7	3	0	8	9	5	7	0	X_{10}
										5	5	2	0	4	5	1	3	0	X_{11}
											9	4	1	8	9	5	7	2	X_{12}
												4	0	3	4	1	2	0	X_{13}
													4	4	4	1	4	2	X_{14}
														13	12	7	12	3	X_{15}
															14	6	11	3	X_{16}
																7	7	2	X_{17}
																	12	3	X_{18}
																		3	X_{19}

б)

Рисунок 8 – q-значення симплексів комплексу: а) $K_Y(X;\lambda)$ – КАІС; б) $K_X(Y;\lambda^{-1})$ – КЗ об'єктам КІІ держави

Також, було проведено експериментальне дослідження методу ідентифікації об'єктів КІІ в авіаційній галузі на основі системи S_{SNS}. Для оцінювання адекватності запропонованого методу було використано розроблений програмний застосунок (рис. 9).

Зміна вхідних даних призвела до відповідної зміни вихідних даних, зокрема $\mathbf{a}_{\text{SNS}}$, $\Gamma\left(\{a_m\},\{p_{m\,m'}\}\right)$, $d_{gi}(a_m,\Phi_{di})$, $\varphi_{gi}(a_m,\Phi_{di})$, $h_{m\,m'}\left(d_{gi}\right)$, $G\left(\{B_{ii}\}\cup\{A_q\}\cup\{C_{ji}\},\{P_{qq'}\}\right)$, $Q_d^q\left(d\left(a_m\right)\right)$, $\mathbf{VEI}_{\text{SNS}}$, що свідчить про коректну роботу розробленого методу в різних умовах.

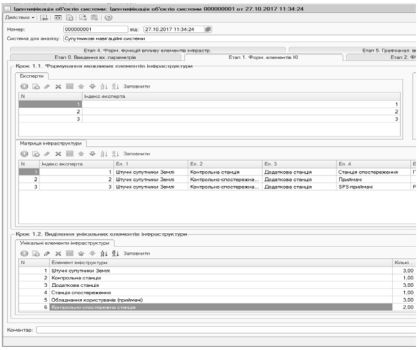


Рисунок 9 – Фрагмент вікна програмного застосунку ідентифікації елементів КІІ

Крім того, було проведено експериментальне дослідження розробленого методу визначення рівня важливості КАІС на прикладі трьох систем: системи обробки даних (S_{SOAD}), бортової системи попередження зіткнень (S_{TCAS}) та глобальної системи резервування (S_{AMDS}).

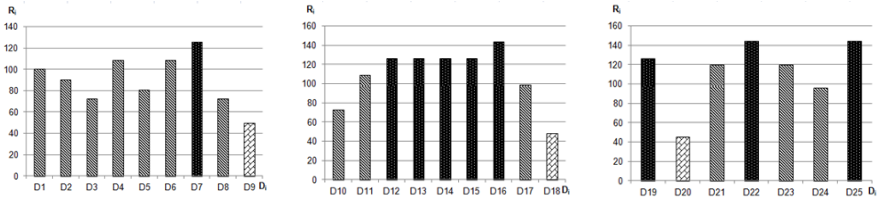
Систематизовані вихідні дані запропонованого методу відображені у табл. 2. Інші вихідні дані отримані на різних етапах реалізації методу, зокрема, матриця критичності, яка за зібраними попередніми даними графічно відображає критичність компонентів системи (етап 7), діаграма Парето, що показує рівень критичності в середині системи та дає можливість порівняти декілька різних систем (етап 9), причинно-наслідкова діаграма Ісікави, що дозволяє виділити пріоритетні напрямки розробки коригувальних заходів (етап 10) та відповідний перелік коригувальних заходів рекомендованих до імплементації.

Таблиця 2

Фрагмент згенерованого звіту

$\mathbf{S}_i/S_{ij}$ /S_{jk}	C_i	F_i	D_i	E_i	O_i	W_i	R			
							B_1	B_2	B_3	R_i
$\mathbf{S}_{1.4}$	C_1	F_1	D_1	E_1	0	W_1	5	4	5	100
	C_2	F_2	D_2	E_2	0	W_1	3	5	6	90
	C_3	F_3	D_3	E_3	0	W_2	3	4	6	72
	C_4	F_4	D_4	E_4	0	W_3	3	6	6	108
	C_5	F_5	D_5	E_5	0	W_4	2	8	5	80
	C_6	F_6	D_6	E_6	0	W_4	3	6	6	108
	C_7	F_7	D_7	E_7	0	W_5	3	6	7	126
		F_8	D_8	E_8	0	W_6	3	4	6	72
		F_9	D_9	E_9	0	W_7	2	5	5	50
		…		E_{10}						
		F_{15}								

На рис. 10 за допомогою діаграми Парето відображено перелік найбільш критичних переривань роботи досліджуваних систем (S_{SOAD} – переривання D_7 (рис. 10а); S_{TCAS} – переривання D_{12} – D_{16} (рис. 10б); S_{AMDS} – переривання D_{19}, D_{22}, D_{25} (рис. 10в)), а також за кількістю виявлених D_i визначена найбільш критична серед досліджуваних КАІС – S_{TCAS}.



а) *б)* *в)*

Рисунок 10 – Діаграми Парето для систем: а) S_{SOAD}; б) S_{TCAS}; в) S_{AMDS}

Проведене експериментальне дослідження методу оцінювання рівня КБ для галузі КІІ показало, що розрахований рівень КБ може приймати значення $-99\% \le \mathbf{I}_{ratio} \le 99\%$, а

критерієм достатності є значення $0\% \le \mathbf{I}_{ratio} \le 20\%$, що свідчить про необхідний рівень КБ галузі КІІ, або цілої держави (на основі практичних рекомендацій NCSI).

На рис. 11 відображені результати експериментального дослідження зазначеного методу для авіаційної галузі. Для розрахунку кількісних параметрів були введені такі обмеження: $\mathbf{I}_{CS} \ge \mathbf{I}_{ICS}$; $\min \mathbf{I}_{CS} \ge 50\%$; $\min \mathbf{I}_{ICS} = 50\%$. У результаті встановлено, що для авіаційної галузі $\mathbf{I}_{ratio_1} = \mathbf{I}_{CS_1} - \mathbf{I}_{ICS_1} = 7\%$. З метою перевірки адекватності реагування методу на вхідні дані було проведено додаткові експерименти – спочатку зменшено апріорні показники, що характеризують стан КБ: $\mathbf{I}_{ratio_2} = 1{,}5\%$, а потім показники, що характеризують впровадження ІКТ: $\mathbf{I}_{ratio_3} = 17\%$.

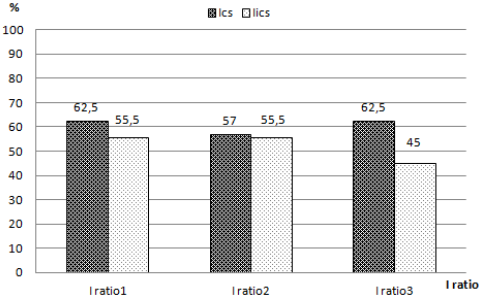


Рисунок 11 – Результати експериментального дослідження методу визначення рівня КБ для авіаційної галузі

Отримані результати (див. рис. 11) підтвердили можливість застосування розробленого методу для розрахунку кількісних параметрів, які характеризують КБ авіаційної галузі.

У **додатках** вміщено акти впровадження результатів дисертаційної роботи і лістинги (фрагменти кодів) розробленого у роботі програмного застосунку.

ВИСНОВКИ

Результатом виконаної дисертаційної роботи є розв'язання актуальної та важливої науково-технічної задачі розроблення методів ідентифікації та оцінювання стану кібербезпеки об'єктів критичної інформаційної інфраструктури авіаційної галузі.

У процесі виконання дисертаційної роботи отримані такі наукові та практичні результати:

1. Проведено аналіз сучасних підходів до ідентифікації та оцінювання стану КБ об'єктів КІІ держави, у результаті чого встановлено, що на сьогодні в Україні відсутній вичерпний перелік об'єктів КІІ та дієві механізми його формування. Також визначено, що відомі підходи до ідентифікації об'єктів КІ орієнтовані, як правило, на економічні, екологічні, техногенні та інші домени безпеки держави та не враховують особливостей КІІ. Існуючі методи визначення рівня критичності не є формалізованими, а методи оцінювання рівня КБ мають низку недоліків, серед яких, відсутність обгрунтування та чіткого кількісного визначення метрик КБ. Проведений аналіз дозволив формалізувати завдання дисертаційного дослідження щодо розробки і вдосконалення методів ідентифікації та оцінювання стану КБ об'єктів КІІ авіаційної галузі.

2. Розроблено уніфіковану модель даних, яка дозволяє формалізувати процес формування переліку об'єктів КІІ держави та визначати їх зв'язність. Також, створено методику, за допомогою якої сформовано перелік об'єктів КІІ авіаційної галузі, у результаті чого (при рівні деталізації $l = 4$) виділено 3 множини категорій, 17 множин систем, 97 множин підсистем, 125 підсистем КАІС. Крім того, використовуючи зазначений перелік, визначено зв'язність КАІС $Q_Y = \{1,1,1,2,2,5,1,1,1,1,1\}$ та КЗ $Q_X = \{1,1,1,2,2,1,1,1,1,1,3,1,1,1\}$, що свідчить про можливість каскадного ефекту КЗ у процесі їх впливу на КАІС. Зазначені результати можуть бути використані відповідними державними органами для формування переліку об'єктів КІІ з метою застосування адекватних методів і засобів захисту.

3. Розроблено метод ідентифікації, який дає можливість визначати (ідентифікувати) елементи галузі КІІ, їх взаємовплив та вплив на функціональні операції КАІС. Також, розроблено і впроваджено спеціальний програмний застосунок, який можна

використовувати для ідентифікації елементів КІІ та визначення їх впливу на функціональні операції, як в авіаційній, так і в інших галузях КІ держави.

4. Удосконалено метод визначення рівня важливості, який дозволяє оцінювати критичність об'єктів КІІ авіаційної галузі як за кількісними, так і за якісними параметрами, а також ранжувати їх для адекватного застосування коригувальних заходів. На основі цього методу створено відповідну методику визначення рівня важливості об'єктів КІІ, яка дає змогу кількісно оцінювати рівень важливості КАІС різних категорій та їх компонентів.

5. Розроблено метод оцінювання рівня КБ, який дає можливість розрахувати кількісні параметри, що характеризують захищеність певної галузі чи КІІ держави в цілому. У результаті проведеного експериментального дослідження встановлено, що для вітчизняної авіаційної галузі, як складової КІ держави, рівень КБ становить 7% (при значенні індексів: КБ – 62,5%, ІКТ – 55,5%).

6. На основі запропонованої методики з використанням розробленого спеціалізованого програмного застосунку, проведено експериментальне дослідження і верифіковано отримані у роботі методи та модель. Результати дисертації впроваджені і використовуються у діяльності ТОВ «Акссонсофт» (акт від 17.04.2018), ДержНДІ Спецзв'язку (акт від 07.02.2017), ІПМЕ ім. Г.Є. Пухова НАН України (акт від 11.04.2017), а також у навчальному процесі кафедри безпеки інформаційних технологій НАУ (акт від 15.12.2017) для підвищення ефективності підготовки фахівців з КБ.

ПУБЛІКАЦІЇ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. V. Sydorenko, T. Zhmurko, Yu. Polishchuk, S. Gnatyuk, «Data Model for Forming Critical Infrastructure Objects and Determining its Connectivity», Inzynier XXI wieku, Monografia, Bielsko-Biala, Poland : ATH, p. 329-350, 2017.

2. Z. Hu, Yu. Khokhlachova, V. Sydorenko, I. Opirskyy «Method for Optimization of Information Security Systems Behavior under Conditions of Influences», *International Journal Intelligent Systems and Applications,* № 12, p. 46-58, 2017.

3. Z. Hu, V. Gnatyuk, V. Sydorenko, R. Odarchenko, S. Gnatyuk «Method for Cyberincidents Network-Centric Monitoring in Critical Information Infrastructure», *International Journal of Computer Network and Information Security*, Vol. 9, № 6, June 2017, p. 30-43, 2017.

4. Aleksander M., Odarchenko R., Kredentsar S., Kozhokhina O., Gnatyuk V., Sydorenko V. «Informational and Functional Reliability Model for Air Navigation System Operator», *TTS*, Badania, №12, p. 287-292, 2016.

5. С. Гнатюк, М. Рябий, В. Лядовська, «Визначення критичної інформаційної інфраструктури та її захисту: аналіз підходів», *Зв'язок*, №4, С. 3-7, 2014.

6. С. Гнатюк, В. Сидоренко, О. Дуксенко, «Сучасні підходи до виявлення та ідентифікації найбільш важливих об'єктів критичної інфраструктури», *Безпека інформації*, Том 21, №3, с. 269-275, 2015.

7. Л. Щербак, С. Гнатюк, В. Сидоренко, О. Шаховал, «Метод визначення рівня важливості об'єктів критичної інформаційної інфраструктури в галузі цивільної авіації», *Безпека інформації*, Том 23, №1, с. 27- 38, 2017.

8. В. Сидоренко, С. Гнатюк, О. Юдін, «Експериментальне дослідження методу визначення рівня важливості об'єктів критичної інформаційної інфраструктури в галузі цивільної авіації», *Захист інформації*, Том 19, №2, с. 155-172, 2017.

9. С. Гнатюк, В. Сидоренко, Н. Сейлова, «Універсальна модель даних для формування переліку об'єктів критичної інформаційної інфраструктури держави», *Безпека інформації*, Том 23, №2, с. 80-91, 2017.

10. С. Гнатюк, В. Кінзерявий, В. Сидоренко, «Метод ідентифікації об'єктів критичної інформаційної інфраструктури в авіаційній галузі», Information technology and security, July-December 2017. Vol. 5. Iss. 2, p. 27- 39, 2017.

11. В. Сидоренко, А. Положенцев, С. Гнатюк, «Метод оцінювання рівня кібербезпеки галузі критичної інформаційної інфраструктури держави», Вісник інженерної академії України, Вип. 42, с. 81- 89, 2017.

12. С. Гнатюк, В. Лядовська, «Критерії визначення елементів критичної інфраструктури держави», *Матеріали XXIII всеукр. наук.-практ. конф. «Інноваційний потенціал світової науки — XXI сторіччя»*. Запоріжжя: Вид-во ПГА, с. 55-57, 2013.

13. С. Гнатюк, В. Лядовська, «Підходи до визначення критичної інфраструктури держави», *Матеріали наук.-практ. конф. «Механізми управління безпекою підприємств в сучасних умовах господарювання»,* м. Київ, 5 грудня 2013 р., с. 83-84, 2013.

14. С. Гнатюк, В. Лядовська, «Ідентифікація об'єктів критичної інфраструктури держави», *Матеріали наук.-практ. конф. «Актуальні проблеми управління інформаційною безпекою держави»,* м. Київ, 20 березня 2014 р., с. 48-52, 2014.

15. В. Лядовська, «Методи та критерії ідентифікації об'єктів критичної інфраструктури держави», *Матеріали VII міжнар. наук.-практ. конф. «Інтегровані інтелектуальні робототехнічні комплекси (ІПРТК-2014)»,* м. Київ, 19-20 травня 2014 р., с. 356-358, 2014.

16. S. Gnatyuk, M. Ryabyy, V. Sydorenko, «Complex approach to ensure civil aviation cybersecurity», *Междунар. науч. конф.: «Украйна – България – Европейски Съюз: съвременно състояние и перспективи»,* Варна – Херсон, 11-17 сентября 2014 г., с. 253-257, 2014.

17. S. Gnatyuk, V. Sydorenko, «Criteria for the identification of critical infrastructures of the state», *The VI world congress «Aviation in the XXI-st century. Safety in Aviation and Space Technologies»,* Kyiv, September 23-25, 2014, V. 1, p. 1.11.68-1.11.71, 2014.

18. С. Гнатюк, В. Сидоренко, «Критична інфраструктура держави», *Матеріали XV міжнар. наук.-практ. конф. молодих учених і студентів «ПОЛІТ-2015. Сучасні проблеми науки»,* м. Київ, 8-9 квітня 2015 р., с. 131, 2015.

19. В. Сидоренко, «Методи виявлення критично важливих об'єктів інфраструктури держави», *Матеріали VIII міжнар. наук.-практ. конф. «Інтегровані інтелектуальні робототехнічні комплекси (ІПРТК-2015)»,* м. Київ, 18-19 травня 2015 р., с.279-281 , 2015.

20. С. Гнатюк, В. Сидоренко, «Огляд методів оцінювання критично важливих об'єктів», *Матеріали IV всеукр. наук.-практ. конф. «Проблеми та перспективи розвитку авіації та космонавтики»,* м. Київ, 28-29 жовтня 2015 р., с. 110, 2015.

21. В. Сидоренко, М. Александер, А. Наджі, «Сучасні підходи до визначення та ідентифікації критичної інформаційної інфраструктури», *Матеріали наук.-практ. конф. «Актуальні питання забезпечення кібернетичної безпеки та захисту інформації»,* м. Київ, 24-27 лютого 2016 р., с. 134-137, 2016.

22. С.О. Гнатюк, Р.С. Одарченко, В.М. Сидоренко «Аналіз методів розрахунку критичності інформаційних систем», *Матеріали IX міжнар. наук.-практ. конф. «Інтегровані інтелектуальні робототехнічні комплекси (ІПРТК–2016)»,* 17-18 травня 2016 р., К. : НАУ, с. 284-286, 2016.

23. В. Сидоренко, А. Оган, «Методи розрахунку критичності інформаційних систем в контексті оцінювання ризиків інформаційної безпеки», *Матеріали VI міжнар. наук.-техн. конф. «Безпека інформаційних технологій (ITSEC–2016)»,* 17-19 травня 2016 р., К.: НАУ, с. 123-124, 2016.

24. В. Сидоренко, «Способи відображення результатів оцінювання рівня важливості об'єктів критичної інфраструктури», *Матеріали XVII міжнар. наук.-практ. конф. молодих учених і студентів «ПОЛІТ-2017. Сучасні проблеми науки»,* м. Київ, 5-7 квітня 2017 р., С. 102-103, 2017.

25. В. Сидоренко, В. Гнатюк, В. Лукашенко, «Підхід до визначення рівня важливості об'єктів критичної інфраструктури в галузі цивільної авіації», *Матеріали III міжнар. наук.-практ. конф. «Актуальні питання забезпечення кібернетичної безпеки та захисту інформації»,* м. Київ, 22-25 лютого 2017 р., с.155-157 , 2017.

26. А. Положенцев, В. Сидоренко, «Метод визначення рівня кібербезпеки об'єктів критичної інфраструктури держави», *Матеріали XVIII міжнар. наук.-практ. конф. молодих учених і студентів «ПОЛІТ-2018. Сучасні проблеми науки»,* м. Київ, 4-6 квітня 2018 р., с. 102-103, 2018.

АНОТАЦІЯ

Сидоренко В.М. Методи ідентифікації та оцінювання стану кібербезпеки об'єктів критичної інформаційної інфраструктури авіаційної галузі. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 21.05.01 «Інформаційна безпека держави». – Національний авіаційний університет, Київ, 2018.

Дисертаційна робота присвячена розв'язанню актуальної науково-технічної задачі розроблення методів ідентифікації та оцінювання стану кібербезпеки (КБ) об'єктів критичної інформаційної інфраструктури (КІІ) авіаційної галузі. У роботі проведено аналіз сучасних підходів до ідентифікації та оцінювання стану КБ об'єктів КІІ держави, що дозволив визначити їх недоліки і формалізувати завдання наукового дослідження щодо розробки і вдосконалення методів ідентифікації та оцінювання стану КБ об'єктів КІІ авіаційної галузі. Розроблено уніфіковану модель даних, яка дозволяє формалізувати процес формування переліку об'єктів КІІ держави та визначити їх зв'язність (співвідношення *q*-зв'язків множин кіберзагроз (КЗ) та критичних авіаційних інформаційних систем (КАІС)). Крім того, створено методику, яка дозволяє формувати перелік об'єктів КІІ певної галузі та на загальнодержавному рівні. Розроблено метод ідентифікації, який дає можливість визначити елементи галузі КІІ, їх взаємовплив та вплив на функціональні операції КАІС. Також, розроблено і впроваджено спеціальний програмний застосунок, який можна використовувати для ідентифікації елементів КІІ та визначення їх впливу на функціональні операції. Удосконалено метод визначення рівня важливості, який дозволяє оцінювати критичність об'єктів КІІ авіаційної галузі та ранжувати їх для адекватного застосування коригувальних заходів. Розроблено метод оцінювання рівня КБ, який дає можливість розрахувати кількісні параметри, які характеризують захищеність певної галузі чи КІІ держави в цілому. На основі запропонованої методики та розробленого спеціалізованого програмного застосунку проведено експериментальне дослідження і верифіковано отримані у роботі методи та модель. Результати дисертації впроваджені і використовуються у діяльності ТОВ «Акссонсофт», ДержНДІ Спецзв'язку, ІПМЕ ім. Г.Є. Пухова НАН України, а також у навчальному процесі кафедри безпеки інформаційних технологій НАУ для підвищення ефективності підготовки фахівців з КБ.

Ключові слова: кібербезпека, критична інфраструктура, критична інформаційна інфраструктура, модель даних, метод ідентифікації, авіаційна галузь, критичні авіаційні інформаційні системи.

АННОТАЦИЯ

Сидоренко В.М. Методы идентификации и оценки состояния кибербезопасности объектов критической информационной инфраструктуры авиационной отрасли. – Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 21.05.01 «Информационная безопасность государства». – Национальный авиационный университет, Киев, 2018.

Диссертационная работа посвящена решению актуальной научно-технической задачи разработки методов идентификации и оценки состояния кибербезопасности (КБ) объектов критической информационной инфраструктуры (КИИ) авиационной отрасли. В работе проведен анализ современных подходов к идентификации и оценке состояния КБ объектов КИИ государства, в результате чего установлено, что на сегодня в Украине отсутствует исчерпывающий перечень объектов КИИ и действенные механизмы его формирования. Также определено, что известные подходы к идентификации объектов критической инфраструктуры (КИ) ориентированы, как правило, на экономические, экологические, техногенные и другие домены безопасности государства и не учитывают особенностей КИИ. Существующие методы определения уровня критичности не являются формализованными, а методы оценки уровня КБ имеют ряд недостатков, среди которых, в частности, отсутствие обоснования и четкого количественного определения метрик КБ. Проведенный анализ позволил формализировать задачи диссертационного исследования относительно разработки и совершенствования методов идентификации и оценки состояния КБ объектов КИИ

авиационной отрасли. Разработана унифицированная модель данных, которая позволяет формализовать процесс формирования перечня объектов КИИ государства и определять их связность. Также, создана методика, с помощью которой сформирован перечень объектов КИИ авиационной отрасли, в результате чего (при уровне детализации $l = 4$) выделено 3 множества категорий, 17 множеств систем, 97 множеств подсистем, 125 подсистем критических авиационных информационных систем (КАИС). Кроме того, используя указанный перечень, определена связность КАИС и киберугроз (КУ), которая свидетельствует о возможности каскадного эффекта КУ в процессе их влияния на КАИС. Указанные результаты могут быть использованы соответствующими государственными органами для формирования перечня объектов КИИ с целью применения адекватных методов и средств защиты. Разработан метод идентификации, позволяющий определять элементы отрасли КИИ, их взаимное влияние и влияние на функциональные операции КАИС. Также, разработано и внедрено специальное программное приложение, которое можно использовать для идентификации элементов КИИ и определения их влияния на функциональные операции как в авиационной, так и в других отраслях КИ государства.

Усовершенствован метод определения уровня важности, который позволяет оценивать критичность объектов КИИ авиационной отрасли как по количественным, так и по качественным параметрам, а также ранжировать их для адекватного применения корректирующих мер. На основе этого метода создана соответствующая методика определения уровня важности объектов КИИ, которая позволяет количественно оценивать уровень важности КАИС различных категорий и их компонентов. Разработан метод оценки уровня КБ, который дает возможность рассчитать количественные параметры, характеризующие защищенность определенной отрасли или КИИ государства в целом. В результате проведенного экспериментального исследования установлено, что для отечественной авиационной отрасли, как составляющей КИ государства, уровень КБ составляет 7% (при значении индексов: КБ – 62,5%, ИКТ – 55,5%).

На основе предложенной методики с использованием разработанного специализированного программного приложения, проведено экспериментальное исследование и верифицированы полученные в работе методы и модели. Результаты диссертации внедрены и используются в деятельности ООО «Акссонсофт», Государственном научно-исследовательском институте специальной связи и защиты информации, Институте проблем моделирования в энергетике им. Г.Е. Пухова НАН Украины, а также в учебном процессе кафедры безопасности информационных технологий НАУ для повышения эффективности подготовки специалистов по КБ.

Ключевые слова: кибербезопасность, критическая инфраструктура, критическая информационная инфраструктура, модель данных, метод идентификации, гражданская авиация, критические авиационные информационные системы.

ABSTRACT

Sydorenko V. Methods for critical information infrastructure objects identification and cybersecurity assessment in aviation. – Manuscript.

Thesis for a Candidate of Technical Science degree in specialty 21.05.01 «Information security of the state». – National Aviation University, Kyiv, 2018.

This thesis is devoted to solving actual scientific and technical problem of developing methods for critical information infrastructure (CII) objects identification and cybersecurity (CS) assessment. In this work modern approaches to CII objects identification and CS assessment was analyzed, it allowed to identify their shortcomings and formalize scientific tasks of the research, regarding to development and improvement of methods for CII objects identification and CS assessment. A unified data model is developed, that allows formalizing the process of creating a CII objects list for the state, and determine their connectivity (the ratio of q-bonds of cyber threats and the critical aviation information system (CAIS) sets). In addition, a technique was developed,

which allows creating a CII objects list both for particular sphere and national level. Method for identification was developed, and it allows identifying CII sphere elements, their influence on functional CAIS operations. Also, a special software application has been developed and implemented, which can be used to identify CII elements and determining their influence on functional operations. Method for determining importance level was improved, which allows evaluating the CII objects criticality in aviation, and rank them for corrective measures adequate use. Method for CS assesment was developed, it gives opportunity to calculate the quantitative parameters, which characterize the security of a particular sphere or CII of the state as a whole. Based on proposed research technique and developed software application, an experimental study was carried out and verified developed methods and model. The results of the thesis were implemented and used in the activity of following companies: AxxsonSoft, State Service of Special Communications and Information Protection of Ukraine, Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine, and also at IT-Security Academic Department of National Aviation University in educational process to increase the efficiency of training specialists in CS.

Key words: cybersecurity, critical infrastructure, critical information infrastructure, data model, identification method, aviation, critical aviation information systems.