Хмельницький національний університет

Факультет інформаційних технологій

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему

Метод захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

КРМКБ.220189.22.01.17 ПЗ

Виконав: студент 2 курсу, група КБм-22-1 _____ Малицький Т.Б.
Підпис

Керівник доц., к.т.н, доцент _____ Чешун В.М.
Підпис

Нормоконтролер старший викладач _____ Мостовий С.В.
Підпис

До захисту допускаю:
Зав. кафедри кібербезпеки, к.т.н., доц _____ Кльоц Ю.П.
Підпис

11 12 2023 р.

Хмельницький, 2023

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Освітній рівень Магістр

Галузь знань 12 Інформаційних технологій

Спеціальність 125 Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ

Зав. кафедри Ю.П. Кльоц

"30" 08 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Малицькому Тарасу Борисовичу
Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Метод захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри

Керівник роботи Чешун Віктор Миколайович
Прізвище, ім'я, по батькові, науковий ступінь, вчене звання
кандидат технічних наук, доцент
Затверджена наказом № 30 ректора університету, додаток №25 від 15.08.2023

2. Строк подання студентом проекту (роботи) на кафедру 15.11.2023

3. Вихідні дані до проекту (роботи) Підвищення ефективності технології захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу, застосування імовірнісних оцінок критеріїв довіри в керуванні правами доступу

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Вступ. Дослідження технологій і методів захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу. Постановка задачі дослідження. Математична модель методу. Алгоритмічна реалізація методу. Апробація отриманих результатів. Висновки.

5. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали і посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Мостовий С.В. старший викладач кафедри		

6. Дата видачі завдання «01» вересня 2023р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Вибір напряму дослідження і узгодження тематики КРМ з керівником	01.06.2023	
2	Ознайомлення з предметною областю; формулювання мети і задач дослідження; визначення об'єкта і предмета дослідження	04.09.2023	
3	Робота над розділом 1 – аналіз відомих моделей, методів за темою; постановка задачі	18.09.2023	
4	Робота над розділом 2 – розробка моделей і методів для вирішення поставленої задачі	02.10.2023	
5	Робота над розділом 3 – розробка алгоритмів і технологій, їх аналіз	16.10.2023	
6	Робота над розділом 4 – апробація запропонованих рішень	06.11.2023	
7	Робота над науковою публікацією	10.11.2023	
8	Узгодження отриманих результатів, оформлення пояснювальної записки згідно вимог	15.11.2023	
9	Попередній захист роботи	17.11.2023	
10	Захист роботи на засіданні ЕК	06.12.2023	

Студент Підпис Т.Б. Малицький Ініціали, прізвище

Керівник проекту (роботи) Підпис В.М. Чешун Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: Метод захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри

Автор роботи: Малицький Тарас Борисович

Керівник роботи: к.т.н., доц. Чешун Віктор Миколайович

Загальний обсяг роботи: 83 сторінки, 12 рисунків, 2 додатки, 54 посилання.

Ключові слова: захист інформації, корпоративна мережа, критерій довіри.

Одним з ключових заходів забезпечення інформаційної безпеки корпоративних мереж є проведення моніторингу та аналізу активності мережі з метою блокування шкідливих дій відносно її ресурсів. Систематичний контроль мережі та виявлення можливих загроз дозволяють оперативно реагувати на кібератаки та аномальну активність, запобігаючи можливим інцидентам.

В роботі представлено метод захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри, що включає в себе математичну модель, основні положення та загальну концепцію методу, реалізацію концепції в термінах математичної моделі, узагальнений і деталізований алгоритми реалізації методу, а також презентацію та апробацію роботи методу.

1.12.2023

ANNOTATION

Theme of qualification work: Method of protecting information resources of a corporate network from unauthorized access based on probabilistic estimates of trust criteria

Author of the work: Malytskyi Taras Borysovych

Mentor: Ph.D. Cheshun Viktor Mykolaiovych

Total volume of work: 83 pages, 12 figures, 2 appendices, 54 links.

Keywords: information protection, corporate network, trust criterion.

One of the key measures to ensure the information security of corporate networks is the monitoring and analysis of network activity in order to block malicious actions against its resources. Systematic monitoring of the network and detection of possible threats allow prompt response to cyber attacks and abnormal activity, preventing possible incidents.

The work presents a method of protecting information resources of the corporate network from unauthorized access based on probabilistic assessments of trust criteria, which includes a mathematical model, the main provisions and general concept of the method, implementation of the concept in terms of a mathematical model, generalized and detailed algorithms for implementing the method, as well as a presentation and approbation of the method.

1.12.2023

ЗМІСТ

ВСТУП

Корпоративна мережа є інфраструктурою, що об'єднує комп'ютери, пристрої та інші обчислювальні ресурси в межах підприємства чи організації [1]. Вона створюється для спільного використання даних, ресурсів та програмного забезпечення серед працівників та відділів. Корпоративні мережі є основою для сприяння комунікації та співпраці всередині організації, забезпечуючи ефективну обробку та обмін даними, спільний доступ до ресурсів та забезпечення захисту важливої інформації.

В умовах все більшого поширення та інтелектуалізації цифрових технологій та зростання кіберзагроз безпека корпоративних мереж стає важливою складовою сучасного бізнесу. Досягнення ефективної безпеки корпоративних мереж вимагає комплексного підходу, враховуючи технологічні інновації та ретельний аналіз потенційних загроз [2]. Технологічні інновації охоплюють сукупність організаційних та програмно-апаратних безпекових заходів [3,4]: міжмережеві екрани, антивірусне програмне забезпечення, шифрування даних, аутентифікація та авторизація, навчання персоналу, регулярні оновлення та патчі, резервне копіювання та відновлення даних, моніторинг та аналіз активності мережі.

Одним із ключових заходів інформаційної безпеки корпоративних мереж є моніторинг та аналіз активності мережі та блокування шкідливих дій з її ресурсами [5]. Постійний моніторинг мережі і виявлення загроз допомагають вчасно реагувати на кібератаки та аномальну активність, запобігаючи можливим інцидентам. Проблема бокування шкідливих дій полягає не безпосередньо в операції блокування, а у прогнозуванні зловмисності дій, тобто, в оцінці «довіри» до ініціатора цих дій. Довіра в інформаційній безпеці є ключовим аспектом для забезпечення захисту конфіденційної інформації та інфраструктури [5]. Щоб оцінити рівень довіри в інформаційній безпеці потрібні критерії визначення, наскільки ефективно застосовуються заходи безпеки та враховуються ризики.

Проведені дослідження свідчать на користь використання в якості критерію довіри суб’єктів взаємодії в інформаційному просторі корпоративної мережі імовірнісного показника, що формується на основі накопичуваної статистики попередньої діяльності кожного суб’єкта із урахуванням зафіксованих випадків шкідливої активності відносно загального показника активності.

Мета кваліфікаційної роботи полягає у вдосконаленні технологій захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу за рахунок оцінки імовірності виникнення загроз і попередження несанкціонованих дій користувачів на основі накопичуваних статистичних даних.

Об'єктом дослідження є процеси захисту інформаційних ресурсів корпоративної мережі та управління правами доступу користувачів.

Предметом дослідження є методи і моделі динамічного адаптивного управління правами доступу користувачів до інформаційних систем корпоративної мережі на основі статистичних даних.

Щоб реалізувати програму досліджень необхідно:

а) виявити перспективні напрямки та способи вдосконалення захисту інформаційних ресурсів корпоративної мережі на основі статистичних даних про дії користувачів;

б) визначити основні положення методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри;

в) розробити математичну модель методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри;

г) розробити алгоритми реалізації методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри;

д) здійснити апробацію запропонованих теоретичних і алгоритмічних рішень.

Методи дослідження базуються на положеннях інформаційної безпеки,

теорії аутентифікації і управління доступом, теорії ймовірностей і математичної статистики, теорії множин.

Наукова новизна отриманих результатів:

1. Запропоновано оригінальну концепцію реалізації методу захисту інформаційних ресурсів корпоративної мережі в термінах математичної моделі;

2. Запропоновано спосіб формування на основі накопичуваних статистичних даних імовірнісних показників критеріїв довіри і їх використання для динамічного адаптивного управління правами доступу користувачів до інформаційних ресурсів корпоративної мережі.

Практична значимість отриманих результатів полягає у визначенні положень і розробці алгоритмів методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу, який забезпечує попередження загроз від дій користувачів з зафіксованими порушеннями політики безпеки роботи в мережі.

Публікації. За темою магістерської роботи опубліковано тези доповідей на 2-х міжнародних та 1-й Всеукраїнській науково-практичних конференціях, підготовлена і прийнята до видання стаття у фаховому журналі.

1 ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ І МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ КОРПОРАТИВНОЇ МЕРЕЖІ

1.1 Корпоративні мережі як об’єкт інформаційної безпеки

Корпоративна мережа визначається як мережа, призначена для забезпечення ефективної роботи певного підприємства, що володіє нею [2]. При побудові корпоративної інформаційної системи (мережі тощо) першочергово слід враховувати, що будь-яка організація представляє собою складну систему, яка складається з взаємодіючих елементів або підрозділів. Кожен із цих підрозділів може мати свою власну структуру та функціональну специфікацію. Ці елементи взаємодіють як функціонально, виконуючи свої завдання в рамках загального бізнес-процесу, так і інформаційно, обмінюючись документами, факсами, письмовими та усними розпорядженнями та іншою інформацією. Більше того, ці елементи організації взаємодіють з зовнішніми системами, і ця взаємодія може бути як інформаційною, так і функціональною. Цей підхід до розгляду організації та її внутрішньої структури є загальноприйнятним та релевантним для різних сфер діяльності [3]. Він стосується як урядових установ, так і комерційних організацій, таких як банки, промислові підприємства, а також фірми з інших галузей. Цей підхід відображає складність та важливість внутрішньої та зовнішньої взаємодії в сучасному бізнесі та організаційному управлінні з точки зору інформатизації та автоматизації тощо.

Корпоративні мережі мають декілька ключових характеристик:

- розподілена інфраструктура;
- загальні ресурси;
- централізоване управління;
- механізми безпеки;
- використання VPN та інших технологій.

Розподілена інфраструктура корпоративних мереж означає, що вони можуть включати в себе різні офіси, філії, відділення та інші віддалені локації, які об'єднуються в єдину мережу для обміну даними та ресурсами [3].

Як правило, корпоративні мережі мають централізовану структуру управління, яка дозволяє адміністраторам керувати, моніторити та керувати всіма аспектами мережі з одного центрального пункту [4]. Корпоративна мережа може включати в себе різноманітні сервіси та інфраструктуру, спрямовані на підтримку бізнес-процесів та забезпечення зручного обміну інформацією всередині підприємства. Це дає можливість підприємствам ефективно впоратися зі своїми потребами у роботі з даними та комунікаціями в сучасному цифровому світі.

Для уникнення можливих проблем з корпоративною мережею рекомендується керуватись правилами [5]:

– в архітектурі корпоративної мережі доцільно використовувати еталонні архітектурні моделі та концепції стандартних рішень, що допоможе визначити чіткі межі для окремих технічних реалізацій і виконання завдань;

– мінімізувати використання продуктів різних виробників на тих ділянках мережі, де вони взаємодіють;

– надавати перевагу використанню стандартів при реалізації мережевих сервісів та чітко відділяти їх на відповідних рівнях архітектури мережі;

– максимально використовувати стандарти – застосування нестандартних або "draft" протоколів в мережі має бути обмеженим або повністю виключеним, стандартизація допомагає забезпечити більш гладку та сумісну роботу всієї мережевої інфраструктури.

Організація корпоративних мереж є ієрархічною і багаторівневою.

Однією із еталонних архітектурних моделей є трирівнева ієрархічна модель корпоративної мережі (рисунок 1.1) [6]. Трирівнева ієрархічна модель корпоративної мережі є основою для ефективної організації і управління мережевою інфраструктурою підприємства. Ця модель передбачає ієрархічний розподіл ролей та функцій мережевих пристроїв для забезпечення оптимальної

продуктивності та ефективного використання ресурсів.

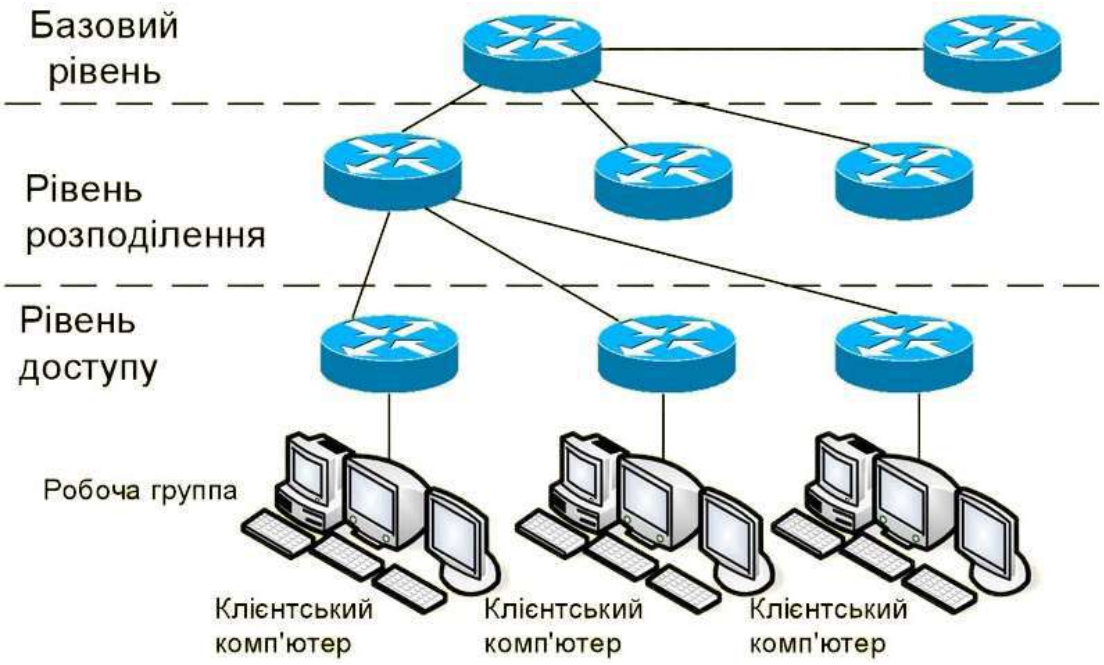


Рисунок 1.1 – Трирівнева ієрархічна модель корпоративної мережі

Така організація корпоративної мережі дозволяє підприємствам забезпечити оптимальну продуктивність, ефективність та масштабованість своєї мережевої інфраструктури, забезпечуючи високу швидкість передачі даних, ефективне керування трафіком та забезпеченням безпеки відповідно до потреб і масштабу підприємства.

Зазвичай корпоративна мережа є географічно розподіленою, об'єднуючи офіси, відділи та інші підрозділи, які можуть знаходитись на значній відстані один від одного. Приклад організації розподіленої корпоративної мережі наведено на рисунку 1.2 [6].

Принципи, на яких базується структура корпоративної мережі, суттєво відрізняються від тих, що застосовуються при створенні локальних мереж. Це вимагає зосередження уваги на вирішенні таких важливих завдань, як забезпечення безпеки передачі даних, ефективне керування ресурсами, а також забезпечення надійного підключення між віддаленими локаціями. Враховуючи ці

особливості, при використанні корпоративної мережі необхідно враховувати різні фактори, включаючи географічне розміщення, рівень безпеки, обсяг та швидкість передачі даних та інші специфічні потреби кожного підрозділу.

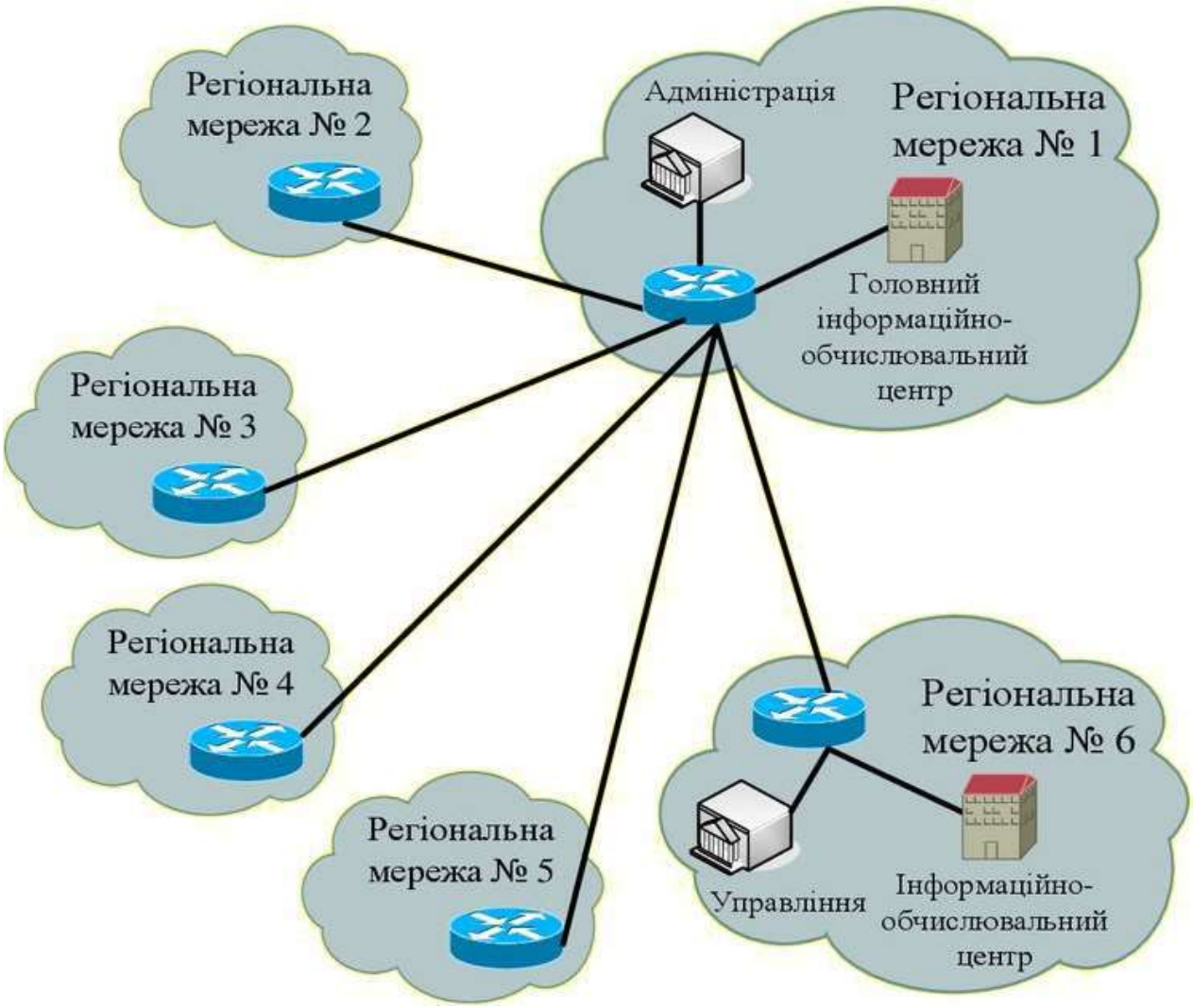


Рисунок 1.2 – Організація розподіленої корпоративної мережі

Для забезпечення безпеки корпоративної мережі застосовуються механізми захисту, що забезпечують для авторизованих користувачів традиційні визначені тріадою CIA критерії конфіденційності, цілісності й доступності даних, а також захищають ресурси корпоративної мережі від зовнішніх загроз та кібератак.

1.2 Методологічні підходи до критеріальної оцінки захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу

Критерії оцінки захисту інформаційних ресурсів дозволяють порівнювати результати незалежних безпекових оцінок в інформаційній системі. Про актуальність критеріїв оцінки свідчить тривала історія їх розробки та вдосконалення, яка не є завершеною і на сьогодні. Деякі критерії оцінки захисту інформаційних ресурсів набули роль міжнародних стандартів (рисунок 1.3 [7]).

Стандарти безпеки комп'ютерних систем, відомі як «Критерії оцінки довірених комп'ютерних систем Міністерства оборони» або «Помаранчева книга» (TCSEC), були розроблені та розвинуті у США протягом 1980-х років. У Європі аналогічні стандарти, відомі як «Критерії оцінки безпеки ІТ» (ITSEC), були створені у 1991 році європейськими країнами (Франція, Німеччина, Великобританія й Нідерланди). Федеральні критерії (FC) Германії були введені в 1992 році. У 1993 році Канада розробила CTCPEC, що став результатом об'єднання двох попередніх стандартів. Крім того, Міжнародна організація зі стандартизації (ISO) в 1990 році почала і продовжує роботу зі створення стандартів і критеріїв оцінки безпеки ІТ для всесвітнього застосування. У 1990 році під егідою ICO та за підтримки державних організацій США, Канади, Великобританії, Франції, Німеччини та Голландії розпочато розробку міжнародного стандарту в галузі оцінки безпеки інформаційних технологій (Загальні критерії оцінки безпеки інформаційних технологій). Перша версія завершена у січні 1996 року й схвалена ICO у квітні 1996 року, 1998 року опублікована друга версія і на її основі у червні 1999 року прийнятий міжнародний стандарт ICO/МЭК 15408. Ці стандарти стали важливим еталоном оцінки безпеки інформаційних технологій та забезпечили загальноприйняті критерії для оцінки рівня захищеності ІТ-продуктів [8,9,10].

У TCSEC були визначені вимоги до засобів захисту інформації в комп'ютерних системах, які опрацьовують критичну інформацію [11,12,13].

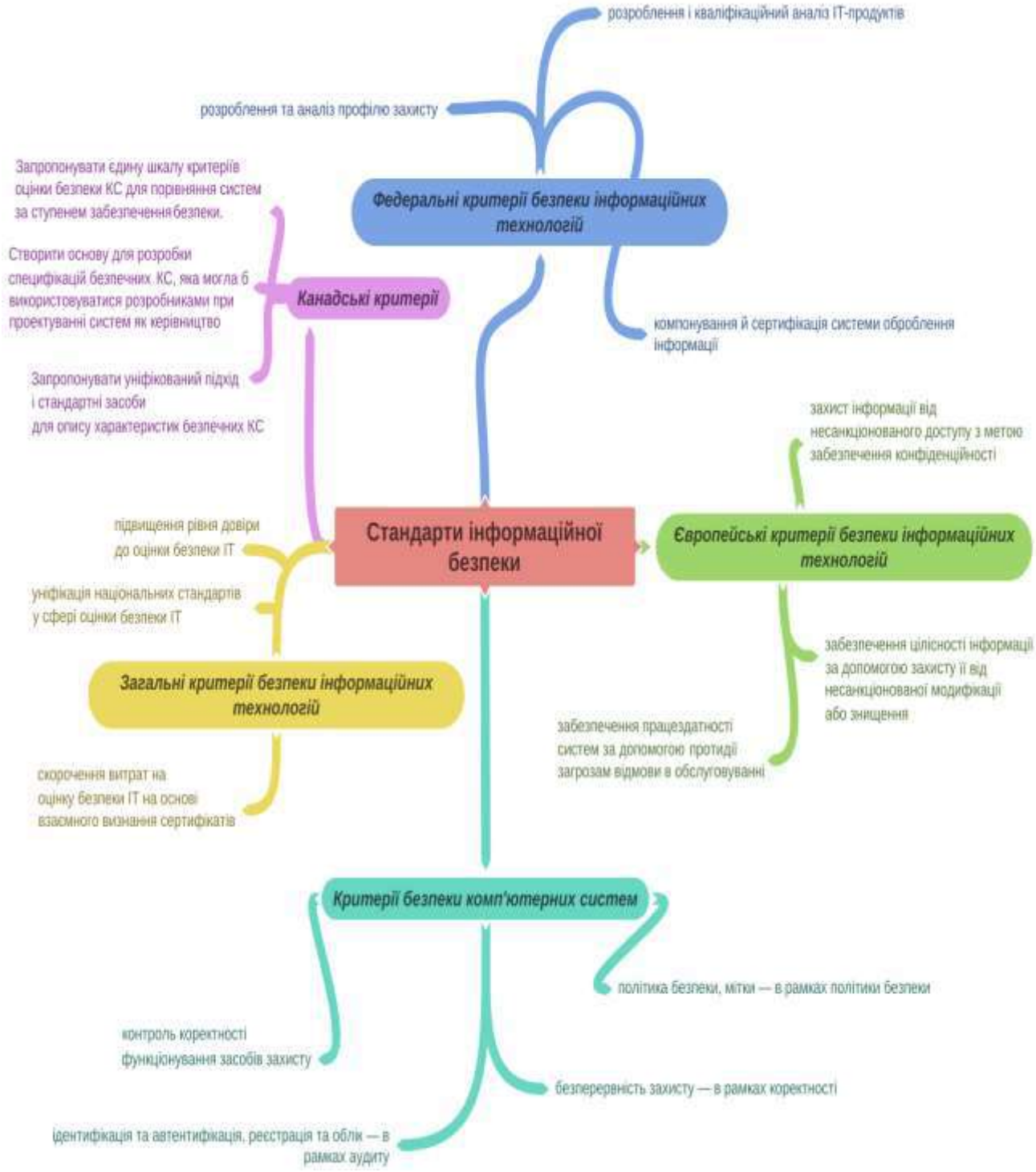


Рисунок 1.3 – Міжнародні критерії-стандарти безпеки IT

TCSEC встановив 4 типи вимог до комп'ютерних систем під час оцінки: вимоги для реалізації політики безпеки, вимоги до обліку використання системи, вимоги до рівня довіри до системи та вимоги до документації продукту. За чотирма рівнями вимог безпеки (D, C, B, A) відбувався розподіл на класи безпеки

(D, C1, C2, B1, B2, B3, A1). Кожному класу був встановлений жорсткий набір критеріїв, що враховував специфічні умови використання конкретних систем.

У 1987 році Національний центр комп'ютерної безпеки США видав інтерпретацію TCSEC для мережевих конфігурацій, що сприяло використанню цих критеріїв в мережевих середовищах і корпоративних тощо.

Ключовим зміненням європейських критеріїв ITSEC від TCSEC була їх підвищена увага до питань забезпечення гарантії безпеки ІТ, враховуючи два аспекти: ефективність та правильність функцій забезпечення безпеки [13,14].

Ефективність оцінювалася з урахуванням критеріїв відповідності набору функцій безпеки загрозам об'єкта оцінки, взаємної взаємодії функцій, простоти їх застосування та можливих наслідків використання відомих слабкі місць захисту.

Коректність оцінювалась через критерії вірності реалізації функцій та механізмів безпеки. Перевірка коректності включала аналіз усього життєвого циклу об'єкта оцінки від етапу проектування до етапу експлуатації та супроводу.

Кінцева оцінка системи в рамках ITSEC формується на основі оцінки критерію мінімальної стійкості механізмів безпеки та рівня гарантії правильності їх функціонування. В ITSEC визнано 7 можливих рівнів гарантії правильності – від E0 до E6.

Критерії оцінки надійності комп'ютерних продуктів Канади CTCPEC [15,16,17] розроблені як національний стандарт безпеки комп'ютерних систем, спрямовані переважно на багатокористувацькі операційні системи і потребують певного узгодження для інших застосувань, таких як бази даних та мережі. Ці критерії спочатку були орієнтовані на широкий спектр комп'ютерних систем. Стандарт встановлював вимоги безпеки, специфікації засобів захисту та сертифікації програмного забезпечення для робочих станцій та багатопроцесорних обчислювальних систем, особистих та багатокористувацьких операційних систем, систем управління базами даних, розподілених, мережевих, вбудованих, об'єктно-орієнтованих та інших систем.

Можливість застосування критеріїв до всіх цих систем визначалася їхнім принципом подвійного представлення вимог безпеки у вигляді функціональних

вимог до засобів захисту та вимог до адекватності їхньої реалізації. Рівень безпеки оцінювався як сукупність критеріїв функціональних можливостей засобів захисту, які характеризуються конфіденційними показниками, що визначали рівень забезпечення безпеки, та одного загального критерія - рівня відповідності реалізації політики безпеки.

Федеральні критерії Германії [18,19,20] висунули галузь використання стандартів на новий етап, почавши розглядати інформаційні технології незалежно від їхнього призначення, зосереджуючись у цьому на відмінностях у характеристиках їхнього експлуатаційного середовища.

Ці критерії включають різноманітні вимог до безпеки ІТ:

– функціональні критерії вимоги, які поділені на вісім класів;

– типові критерії технології розробки продуктів ІТ;

– критерії процесу кваліфікаційного аналізу продуктів ІТ, які включають три групи вимог, що регулюють аналіз, контроль та тестування.

Центральним поняттям концепції інформаційної безпеки в "Федеральних критеріях" є поняття "профілю захисту" (protection profile). Згідно з цими критеріями, профіль захисту є нормативним документом, який регулює всі аспекти безпеки продукту ІТ, включаючи вимоги до його проєктування, технології розробки та кваліфікаційного аналізу. Зазвичай один профіль захисту описує кілька схожих за структурою та призначенням продуктів ІТ. Основна увага у профілі захисту приділяється вимогам до складу засобів захисту та якості їхньої реалізації, а також їх адекватності передбачуваним загрозам безпеці [20].

У «Загальних критеріях» (ЗК) [13,21,22] виконано класифікацію різноманітних функціональних вимог та вимог щодо впевненості у безпеці, визначено структури їхнього групування та принципи цілеспрямованого використання.

Загальні критерії становлять собою методологію та систему формування вимог та оцінки безпеки ІТ. Ця системність проявляється від використання спеціальної термінології та рівнів абстракції для відображення вимог до безпеки

та забезпечення оцінки безпеки на всіх етапах життєвого циклу ІТ-продуктів [23].

Загальні критерії вирізняються найбільш повним і актуальним на сьогоднішній день переліком критеріїв оцінки безпеки ІТ. В ЗК здійснено чітку розмежування вимог безпеки на функціональні вимоги та вимоги щодо довіри до безпеки. Функціональні вимоги охоплюють сервіси безпеки, такі як ідентифікація, аутентифікація, управління доступом й аудит тощо, тоді як вимоги довіри стосуються технології розробки, тестування, аналізу вразливостей, експлуатаційної документації, постачання та супроводу, охоплюючи всі етапи життєвого циклу ІТ-продуктів.

Загальні критерії включають шкалу оціночних рівнів довіри до безпеки, яка може використовуватися для створення різних рівнів впевненості у безпеці продуктів ІТ. Систематизація та класифікація критеріїв за ієрархічними категоріями «клас-сімейство-компонент»-«елемент» з використанням унікальних ідентифікаторів вимог додає зручності у їхньому використанні. Критерії, що належать до різних сімейств та класів, ранжовані відповідно до рівня деталізації та строгості, а також групуються у пакети вимог для забезпечення узгодженості.

Гнучкий підхід до формування критеріїв безпеки для різних типів ІТ-продуктів та умов їх використання забезпечується можливістю цілеспрямованого створення необхідних наборів вимог у вигляді стандартизованих структур, які визначені в ЗК. ЗК відкриті для подальшого розширення набору вимог та можуть включати нові структури та категорії згідно з розвитком технологій та змінами в сфері безпеки.

Згідно з експертними оцінками в галузі кібербезпеки [16,24,25], ЗК відзначаються найвищим рівнем систематизації, повнотою та гнучкістю у деталізації вимог-критеріїв, що робить їх найбільш досконалими серед існуючих стандартів на сьогоднішній день. Особливо важливо відзначити, що завдяки своїй конструкції вони можуть необмежено розвиватися, виступаючи не лише як функціональний стандарт, але й як методологія формування, оцінки та каталогізації вимог безпеки ІТ.

Незважаючи на наявність і постійний розвиток стандартів критеріальної оцінки безпеки ІТ, вони не є всеохоплюючими, що зумовлює потребу та інтерес фахівців з кібербезпеки у неперервному розширенні напрямків досліджень з вдосконалення методів та технологій оцінки якості захисту інформаційних ресурсів корпоративних мереж від несанкціонованого доступу за різними критеріями відповідно до сучасних викликів і технологічних новацій.

В роботі [26] пропонується методика оцінювання ефективності системи інформаційної безпеки міністерства оборони та ЗСУ. Блок-схема реалізації методики оцінювання ефективності системи інформаційної безпеки представлена на рисунку 1.4.

Методика ґрунтується на удосконаленій системі критеріїв та показників оцінювання ефективності функціонування системи забезпечення інформаційної безпеки.

Методика базується на вдосконаленій системі критеріїв та показників для оцінки ефективності інформаційної безпеки [27], організованої з трьох блоків.

У першому блоці, за допомогою експертного методу, визначається потрібний набір вхідних даних для здійснення оцінки ефективності системи із забезпечення інформаційної безпеки.

У другому блоці проводиться комплексна оцінка ефективності одразу за чотирма групами критеріїв.

У третьому блоці результати попередньої оцінки нормованих показників щодо ефективності порівнюються з певним рівнем обмежень. Якщо умова виконується, тоді експерт робить висновок, що досліджувана система виконує свої функції цілком ефективно. В іншому випадку слідує висновок, що додатково мають бути зроблені висновки щодо причин, чому саме досліджувана система не виконує свої функції, та надані практичні рекомендації для підвищення ефективності системи.

Після цих трьох етапів процедура циклічно повторюється для подальшої оцінки.

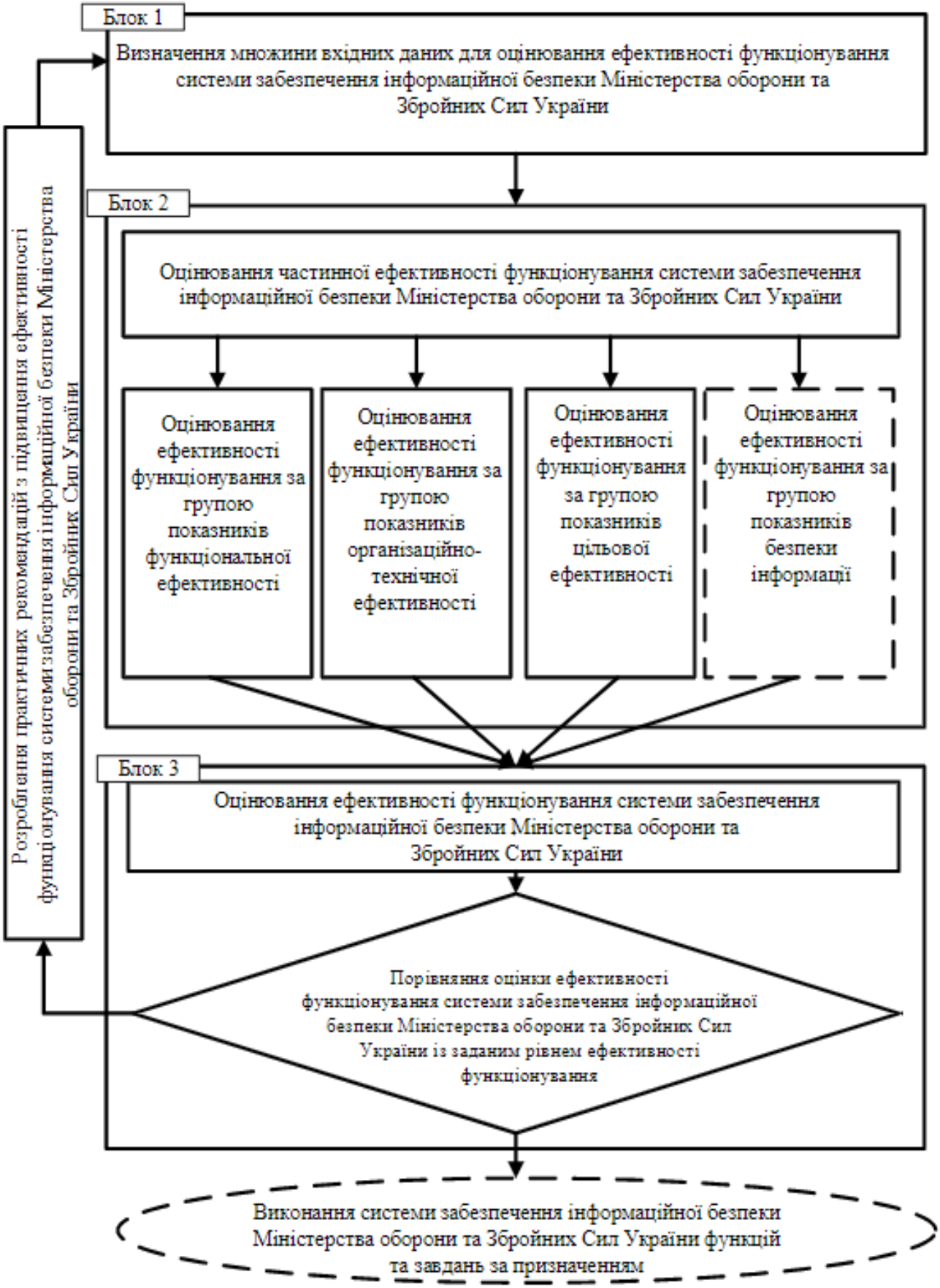


Рисунок 1.4 – Блок-схема методики оцінювання ефективності системи інформаційної безпеки

Автори методики оцінки захищеності інформаційних систем [28] пропонують здійснювати оцінку у 10 етапів:

– визначення категорій, які беруть участь у оцінці;

– упорядкування категорій та розрахунок вагових коефіцієнтів для них;

– упорядкування підгруп кожної категорії та визначення вагових коефіцієнтів для цих підгруп;

– позначення про виконання дій, зазначених у компонентах кожної підгрупи серед категорій, що беруть участь у оцінці;

– створення матриці вагової функції на підставі позначок про виконання;

– розрахунок зв'язків для кожного компонента підгрупи, якщо такі зв'язки передбачені стандартом;

– розрахунок загальних показників для кожної категорії;

– обчислення загального показника;

– розрахунок зв'язків, загальних показників та загального показника для категорій, що беруть участь у оцінці в умовах, коли всі позитивні позначки про виконання дій, зазначених у компонентах кожної підгрупи, присутні;

– порівняння результатів, отриманих на етапах 8 та 9, і формулювання рекомендацій щодо підвищення безпеки оцінюваної інформаційної системи.

Різноманітні критерії оцінювання безпеки мереж та ІТ також розглядають автори багатьох інших наукових публікацій [28-35], що свідчить про актуальність досліджень з захисту інформаційних ресурсів корпоративних мереж від несанкціонованого доступу на основі різноманітних критеріїв оцінок.

Одним із перспективних напрямків оцінки захисту інформаційних ресурсів від несанкціонованого доступу, що активно розвивається, є використання в оцінці критеріїв довіри. Для прикладу, механізм оцінки аудиту SOC 2 [36,37] дозволяє виміряти ефективність функціонування системи безпеки компанії, спираючись на основні стандартів та Критеріїв довірених сервісів. Ці критерії дозволяють компанії визначити ступінь вірогідності, що процеси і системи відповідають встановленим нормам безпеки, конфіденційності, обробки,

конфігурації та доступності даних. Аудит SOC 2 не тільки вимірює дотримання цих стандартів, але і допомагає виявляти можливі слабкі місця та пропонує рекомендації щодо покращення системи безпеки та окремих процесів.

Аудит SOC 2 використовується організаціями для задоволення потреб довіри користувачів, яким потрібна докладна інформація та впевненість в тому, як обслуговуюча організація контролює безпеку, доступність та цілісність обробки своїх систем, а також як вона забезпечує конфіденційність даних, які обробляються цими системами. SOC 2 визначає конкретні критерії довіри для кожного з принципів і обслуговуючі організації повинні відповідати цим критеріям через засоби контролю, які вони впроваджують. Всі оцінки SOC 2 повинні включати принцип безпеки як обов'язковий. Однак, обслуговуючі організації можуть також вибрати додаткові критерії для включення до перевірки SOC 2.

1.3 Постановка задачі

Для вирішення поставлених задач було проведене дослідження корпоративних мереж як об’єкту інформаційної безпеки, в ході якого були проаналізовані принципи організації корпоративних мереж та типові загрози безпеці їх інформаційних ресурсів.

В результаті було встановлено, такі мережі можуть мати різну організацію, але їм властиве централізоване управління, загальні ресурси і обмежене коло користувачів.

Основними типами загроз інформаційним ресурсам корпоративної мережі є внутрішні, які походять від співробітників корпорації і тому управління доступом до інформаційних ресурсів на концепції довіри до співробітників, а саме на основі імовірнісних оцінок критеріїв довіри до користувачів, є перспективним напрямком у вдосконаленні технологій захисту інформаційних ресурсів корпоративної мережі.

Для розробки методу у відповідності до вимог завдання в роботі необхідно:

– розробити математичну модель методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри;

– визначити основні положення методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри;

– розробити алгоритми реалізації методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри;

– здійснити апробацію запропонованих теоретичних і алгоритмічних рішень.

2 МАТЕМАТИЧНА МОДЕЛЬ МЕТОДУ

2.1 Визначення концептуальних положень математичної моделі

При розробці методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри важливою складовою постає математична модель як базис для створення і оцінки ефективності методу.

Першочергово слід визначити концептуальні положення щодо виду і особливостей математичної моделі методу захисту інформаційних ресурсів корпоративної мережі, що потребує аналізу властивостей існуючих моделей і вибору типу моделі для використання у методі.

Загальний аналіз математичних моделей дозволяє дійти висновку, що математичні моделі є важливим інструментом в наукових дослідженнях, інженерії, економіці, соціології та інших галузях знань. Вони дозволяють представити досить складні реальні процеси у вигляді абстрактних залежностей, які можна досліджувати та аналізувати за допомогою математичних методів.

Математичні моделі використовуються для самих різноманітних цілей у багатьох галузях науки, техніки, соціальних задач, що дає можливість аналізувати складні явища і процеси за їх безпосередньої відсутності в дослідницьких операціях.

У залежності від призначення й особливостей конкретно заданого об'єкта дослідження, існують різні класи і типи математичних моделей.

Для вибору моделі метод захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри здійснимо короткий аналіз властивостей математичних моделей.

Аналітичні моделі описуються у вигляді аналітичних функцій або формул, використання яких дозволяє отримувати якісні аналітичні рішення для окремих

класів задач. Аналітичні моделі, зазвичай, застосовуються для аналізу нескладних систем з відомими законами (залежностями) міжкомпонентної взаємодії.

Геометричні моделі базуються на використанні геометричних образів (фігур або просторових моделей тощо) для представлення об'єктів й процесів. Геометричні моделі дозволяють візуально сприймати, аналізувати і розуміти просторові міжкомпонентні відношення між об'єктами у їх взаємодії.

Статистичні моделі використовуються для аналізу випадкових процесів та подій, які, як правило, не можна апріорно описати детальною функціональною залежністю. Статистичні моделі як вид дозволяють враховувати випадковість та й невизначеність вихідних даних.

Ймовірнісні статистичні математичні моделі – підвид статистичних математичних моделей, які використовують ймовірнісні підходи та статистичні методи для аналізу та моделювання випадкових подій, процесів і явищ. До цієї категорії відносяться регресійні моделі (використовуються для вивчення залежностей між змінними та прогнозування майбутніх значень на основі статистичного аналізу взаємозв'язків між змінними і дозволяють встановлювати ступінь впливу однієї або кількох змінних на інші), часові ряди (використовуються для аналізу та прогнозування даних, що залежать від часу, дозволяють виявляти тенденції, циклічність, сезонність та інші регулярні закономірності у часових рядах), Марковські моделі (використовуються для вивчення стохастичних процесів, які задовольняють властивість Маркова, для аналізу ймовірності переходу між станами системи та прогнозування подальшого розвитку процесів), Байєсівські моделі (використовуються для оцінки ймовірності подій на основі апріорних знань та нової інформації і дозволяють враховувати нестачу даних та невизначеність у моделюванні реальних процесів), моделі масового обслуговування (використовуються для аналізу та оптимізації процесів обслуговування, таких як обробка транзакцій, обслуговування клієнтів та інші, дозволяють визначити оптимальні стратегії управління обслуговуванням при великому обсязі запитів) тощо.

Ці ймовірнісні статистичні математичні моделі допомагають вирішувати складні завдання аналізу даних та прогнозування на основі випадкових процесів, що зустрічаються у різних галузях науки та техніки.

Моделі на диференціальних рівняннях використовуються для опису-відображення зміни величин у часі або у просторі. Моделі на диференціальних рівняннях дозволяють аналізувати динаміку систем, що змінюються з плином часу, та вивчати їх стійкість та поведінку у різних умовах.

Імітаційні моделі – різновид моделей, що дозволяють відтворювати реальні процеси або роботу систем у вигляді комп'ютерного програмного забезпечення або алгоритмічно, що дозволяє проводити експерименти та аналізувати різні сценарії без прямого втручання в реальні системи.

Різні типи математичних моделей є інструментом розуміння-передбачення поведінки різноманітних систем і протікання процесів у різних сферах. Для методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри особливої актуальності набувають математичні моделі, застосовувані саме у сфері кібербезпеки.

У сфері кібербезпеки математичні моделі мають своє застосування й відіграють важливу роль для розуміння та при прогнозуванні потенційних загроз, розробці ефективних алгоритмів і стратегій захисту, для виявлення кібератак тощо. Моделі загроз допомагають ідентифікувати потенційні кіберзагрози, оцінювати їх вплив та ризики для інформаційних систем. Вони дозволяють прогнозувати можливі сценарії атак та розробляти стратегії захисту. Моделі доступу у сфері кібербезпеки використовуються для керування доступом до різноманіття інформаційних ресурсів та систем. Моделі доступу визначають права доступу користувачів і використовуються в задачах контролю поведінки користувачів, передбачають аутентифікацію, авторизацію та забезпечують аудит доступу. Моделі управління ризиками допомагають оцінювати та здійснювати керування ризиками, пов'язаними з інформаційною безпекою. Моделі управління ризиками дозволяють ідентифікувати уразливості мережі або іншої

інформаційно-комунікаційної системи, оцінювати можливі наслідки кібератак, розробляти та досліджувати стратегії мінімізації ризиків. Моделі виявлення вторгнень допомагають виявляти аномальні й шкідливі активності у мережі (інформаційній системі тощо). Моделі виявлення вторгнень є основою для синтезу алгоритмів виявлення вторгнень, які можуть реагувати на різні небезпечні дії або події у режимі реального часу. Спеціалізовані моделі шифрування та криптографії використовуються для розробки та криптоаналізу систем шифрування, призначенням яких є забезпечення конфіденційності та цілісності даних у їх транзиті в мережі або іншій інформаційно-комунікаційній системі. Моделі шифрування та криптографії для організації захисту інформації від несанкціонованого доступу використовують, так звані, математичні алгоритми. Моделі аналізу стійкості систем допомагають фахівцям оцінювати стійкість інформаційних систем щодо різних видів кіберзагроз. На моделі аналізу стійкості систем досліджують вразливості системи, результати досліджень допомагають вдосконалити архітектуру системи захисту для запобігання можливим атакам.

Різні призначення математичних моделей допомагають створювати ефективні та надійні стратегії кібербезпеки для захисту інформаційних ресурсів та запобігання кіберзлочинності. Згідно з основною ціллю методу звернемо особливу увагу на моделі кібербезпеки на основі концепції довіри.

Математичні моделі кібербезпеки, що ґрунтуються на концепції довіри, відіграють важливу роль у забезпеченні безпеки та захисту від кіберзагроз й кібератак інформаційних ресурсів комп’ютерних мереж та систем різної складності та топології. Такі математичні моделі базуються на аналізі взаємодії між різними суб'єктами та об'єктами в інформаційному середовищі та визначають ступінь довіри до цих суб'єктів та об'єктів з точки зору інформаційної безпеки ресурсів мережі. Моделі довіри є важливим інструментом в задачах підвищення рівня кібербезпеки та забезпеченні надійного захисту інформаційних систем та мереж від сучасних кіберзагроз та кібератак.

Математичні моделі кібербезпеки, що ґрунтуються на концепції довіри, можна розділити на декілька класів.

Першочергово слід відзначити моделі довіри в мережах передачі даних, які вивчають взаємодію між вузлами мережі передачі даних та визначають рівень довіри до кожного вузла на основі його попередньої поведінки, автентичності та інших параметрів. Моделі довіри в мережах передачі даних допомагають ідентифікувати та ізолювати небезпечні вузли та мінімізувати ризики загалом для мережі передачі даних.

Інший вид моделей кібербезпеки на основі концепції довіри – моделі довіри в системах управління доступом. Моделі довіри в системах управління доступом аналізують і оцінюють довіру до користувачів та визначають їхні права доступу на основі рівня довіри, який надається кожному користувачеві. Вони допомагають обмежувати доступ до конфіденційної інформації та захищати систему від несанкціонованого доступу та кібератак.

Окремим видом моделей кібербезпеки на критеріях довіри є моделі довіри в криптографічних системах. Моделі довіри в криптографічних системах досліджують стійкість криптографічних систем та алгоритмів шифрування на основі рівня довіри до криптографічних ключів та протоколів. Такі моделі довіри допомагають виявляти та усувати потенційні уразливості та забезпечувати надійний захист конфіденційної інформації.

Ще один клас моделей кібербезпеки, що базується на концепції довіри – моделі довіри в системах виявлення вторгнень. Такі моделі вивчають довіру до різних систем виявлення вторгнень та визначають їхню ефективність на основі рівня довіри до якості виявлення загроз. Цей клас моделей допомагає вдосконалювати системи виявлення вторгнень та мінімізувати ризики кібератак.

Завершуючи аналіз класифікуємо математичну модель для використання у методі:

– математична модель методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних

оцінок критеріїв довіри є різновидом статистичних моделей, оскільки використовується для аналізу випадкових процесів та подій у корпоративній мережі, пов’язаних з непередбачуваною поведінкою користувачів цієї мережі, яку апріорно не можна передбачити і тому неможливо наперед описати детальною функціональною залежністю. Саме випадковість і невизначеність вихідних даних щодо можливих дій користувачів інформаційних ресурсів корпоративної мережі є передумовою застосування самого методу і його математичної моделі тощо;

– математична модель створюваного методу є ймовірнісною статистичною моделлю, оскільки передбачається використання ймовірнісних підходів прогнозування-попередження зловмисних дій та статистичних методів аналізу поведінки користувачів;

– в певному аспекті математична модель методу є різновидом моделі управління ризиками, оскільки кінцева ціль застосування пропонованого методу – мінімізація ризиків через ідентифікацію і попередження потенційних загроз від дій користувачів інформаційних ресурсів корпоративної мережі через розмежування і обмеження прав доступу до цих ресурсів;

– математична модель методу є типовою моделлю на концепції довіри, що слідує з визначеної у назві методу методології захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу саме на основі імовірнісних оцінок критеріїв довіри. Математична модель методу базується на аналізі взаємодії між різними суб'єктами (користувачами) та об'єктами (інформаційними ресурсами) в інформаційному середовищі мережі та визначають ступінь довіри до суб'єктів з точки зору інформаційної безпеки;

– математична модель пропонованого методу у категоріюванні математичних моделей кібербезпеки відноситься до підкласу моделей доступу (моделей систем управління доступом), оскільки сам метод призначається для реалізації найбільш ефективних систем управління, які забезпечують керування доступом до інформаційних ресурсів корпоративної мережі і достовірно

контролюють та обмежують доступ підозрілих користувачів до інформації з обмеженим доступом, конфіденційної інформації тощо;

– узагальненням двох останніх пунктів модель пропонованого методу можна ідентифікувати як модель довіри систем управління доступом, оскільки метод орієнтовано на управління доступом через оцінку рівня довіри до користувачів та визначення їхніх прав доступу на основі рівня довіри, який розраховується для кожного користувача;

Отже, концептуально математичну модель методу можна класифікувати як ймовірнісну статистичну модель систем управління доступом на основі концепції (критеріїв) довіри.

2.2 Деталізація математичної моделі методу

Для ефективного застосування математичної моделі методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри, після визначення її виду, концептуальних положень та загальних особливостей, постає необхідність здійснити деталізацію математичної моделі методу, тобто, уточнення і опису усіх її складових.

Першочергово в математичній моделі слід визначити об’єкти і суб’єкти, що вступають у взаємодію при реалізації методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри.

Відповідно до положень Закону України «Про інформацію» [38] як суб'єкти інформаційних відносин розглядаються:

– фізичні особи (посадові особи, а для нашого випадку – користувачі інформаційних ресурсів корпоративної мережі);

– юридичні особи (це організації, які пройшла затверджену законодавством процедуру реєстрації з відповідними правами і обов’язками: підприємства держаної та приватної власності, фірми, корпорації, ФОП, ТОВ тощо [39]);

– об'єднання громадян (добровільні громадські формування, які створюються на основі єдності інтересів з ціллю спільної реалізації самих різноманітних своїх прав і свобод: профспілкові організації, благочинні об'єднання тощо [40]);

– суб'єкти владних повноважень (різноманітні органи державної влади і місцевого самоврядування, а також посадові-службові особи цих органів [41]).

З наведеного переліку суб’єктів інформаційних відносин суб’єктами взаємодії методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри виступають тільки фізичні особи, тобто, посадові особи і співробітники організації-власника корпоративної мережі, якими є користувачі інформаційних ресурсів зазначеної мережі та її адміністратори. Можливість доступу до інформаційних ресурсів корпоративної мережі сторонніх осіб ігноруємо, що має забезпечуватись політикою безпеки організації та розмежуванням прав доступу системи контролю доступу до мережі та мережевих ресурсів.

Таким чином, в математичній моделі методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри нам необхідно ідентифікувати суб’єкти інформаційних відносин, якими є користувачі та адміністратори корпоративної мережі.

Аналіз показує, що найбільш зручним способом представлення в математичній моделі методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри суб’єкти інформаційних відносин є їх ідентифікація елементами теорії множин, тобто, множиною суб’єктів:

$$SUBJECTS:\{Subject_1, Subject_2, \dots, Subject_i, \dots, Subject_k\}; \quad (2.1)$$

де SUBJECTS – множина, що відображує всіх користувачів корпоративної мережі $Subject_i \in SUBJECTS$, якими можуть бути як звичайні користувачі мережі з різними посадовими обов'язками (керівництво, посадові особи, оператори тощо), так і адміністратори цієї мережі.

Відповідно до положень того ж Закону України «Про інформацію» як об'єкт інформаційних відносин розглядається лише інформація, але інформацією є: «будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді».

Тобто, як об'єкт взаємодії методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри виступає інформація, яка збережена (обробляється, транспортується тощо) на матеріальних носіях (обробляється, транспортується матеріальними ресурсами корпоративної мережі тощо) і має відображення в електронному вигляді.

Таким чином, як об'єкт взаємодії методу захисту інформаційних ресурсів корпоративної мережі можуть розглядатися будь-які її інформаційні ресурси, які можуть бути використані як джерело або інструмент несанкціонованого доступу до відображеної в електронному вигляді інформації (бази даних, програмне забезпечення, файлові елементи, накопичувачі даних тощо). Оскільки таких інформаційних ресурсів в корпоративній мережі може бути велика кількість, для ідентифікації об'єктів взаємодії методу доцільно використати також інструментарій теорії множин, тобто, ввести до математичної моделі множину об'єктів інформаційних відносин:

$$OBJECTS:\{Object_1, Object_2, \dots, Object_j, \dots, Object_n\}; \quad (2.2)$$

де OBJECTS – множина, що відображує облікові при реалізації методу як об’єкти інформаційної взаємодії інформаційні ресурси $Object_j \in OBJECTS$ корпоративної мережі, якими можуть бути бази даних, програмне забезпечення, файлові елементи, накопичувачі даних тощо.

Деталізований перелік інформаційних ресурсів корпоративної мережі для формування множини OBJECTS об’єктів інформаційної взаємодії має складати експертна група фахівців з кібербезпеки власника корпоративної мережі або запрошені фахівці-експерти на підставі детального аналізу інформаційних активів корпоративної мережі з урахуванням специфіки економічної та інших видів діяльності замовника.

Для відображення взаємодії об’єктів і суб’єктів інформаційних відносин при реалізації методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри найбільш презентативною і зручною в подальшій обробці є матрична форма представлення даних.

Повертаючись до визначених в попередньому підрозділі пояснювальної записки концептуальних висновків щодо приналежності математичної моделі методу до підкласу моделей доступу (моделей систем управління доступом) через орієнтацію пропонованого методу на реалізацію найбільш ефективних систем управління, які забезпечують керування доступом до інформаційних ресурсів корпоративної мережі і достовірно контролюють та обмежують доступ підозрілих користувачів до інформації з обмеженим доступом, конфіденційної інформації тощо, можна обрати типовий для систем контролю доступу варіант представлення є даних у матричній формі – матрицю доступу.

Типовим прикладом такої матриці є наведена у роботі [42] матриця доступу для використання в дискреційній моделі розмежування прав доступу (рисунок 2.1).

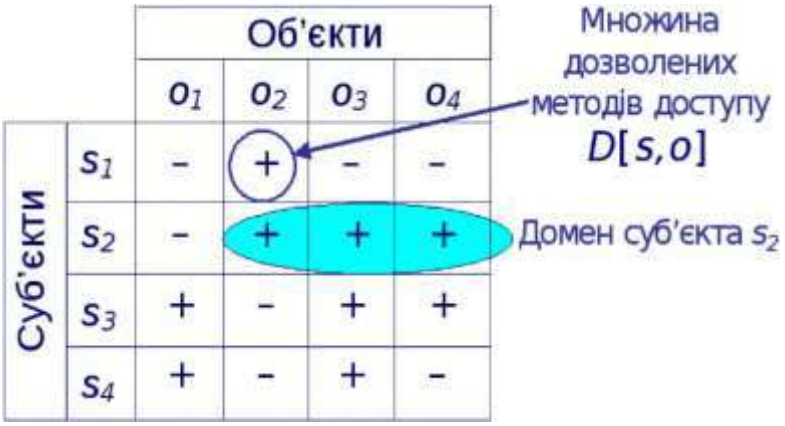


Рисунок 2.1 – Матриця доступу дискреційної моделі розмежування прав

Аналіз потреб методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри дозволяє визначити три варіанти матричного відображення розмежування прав доступу і фіксації здійснених спроб доступу:

– матриця доступу для визначення прав доступу користувачів корпоративної мережі $Subject_i \in SUBJECTS$ (суб'єктів інформаційних відносин) до інформаційних ресурсів мережі $Object_j \in OBJECTS$ (до об'єктів інформаційних відносин);

– матриця фіксації санкціонованих (дозволених) дій користувачів $Subject_i \in SUBJECTS$ корпоративної мережі в полі інформаційних ресурсів $Object_j \in OBJECTS$;

– матриця фіксації спроб (вдалих або невдалих, несанкціонованого доступу тощо) здійснення несанкціонованих (заборонених) дій користувачів $Subject_i \in SUBJECTS$ корпоративної мережі в полі інформаційних ресурсів $Object_j \in OBJECTS$.

Наведений на рисунку 2.1 варіант матриці доступу не є зручним у перелічених застосуваннях при реалізації методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри, тому здійснимо адаптацію матриць доступу відповідно до описаних потреб методу.

Для зручності математичної обробки даних матриці визначення прав доступу користувачів корпоративної мережі $\text{Subject}_i \in \text{SUBJECTS}$ до інформаційних ресурсів мережі $\text{Object}_j \in \text{OBJECTS}$ наведену на рисунку 2.1 матрицю доцільно звести до матриці прав доступу (Matrix Of Access Rights) булевого типу, в якій кожен елемент $AR_{ij} \in \text{MatrixOfAccessRights}$ буде бінарним однорозрядним числом, що визначається за правилом:

$$AR_{ij} = \begin{cases} 0, \text{ якщо суб'єкт } \text{Subject}_i \in \text{SUBJECTS не має} \\ \quad \text{прав доступу до ресурсу } Object_j \in \text{OBJECTS}, \\ 1, \text{ якщо суб'єкт } \text{Subject}_i \in \text{SUBJECTS має} \\ \quad \text{права доступу до ресурсу } Object_j \in \text{OBJECTS}. \end{cases} \quad (2.3)$$

В узагальненому представлені матриця прав доступу множини користувачів корпоративної мережі SUBJECTS до множини облікованих інформаційних ресурсів корпоративної мережі OBJECTS може бути представлена у вигляді:

$$\text{MatrixOfAccessRights} = \begin{vmatrix} AR_{1,1} & AR_{1,2} & \cdots & AR_{1,|\text{OBJECTS}|} \\ AR_{2,1} & AR_{2,2} & \cdots & AR_{2,|\text{OBJECTS}|} \\ \vdots & \vdots & & \vdots \\ AR_{|\text{SUBJECTS}|,1} & AR_{|\text{SUBJECTS}|,2} & \cdots & AR_{|\text{SUBJECTS}|,|\text{OBJECTS}|} \end{vmatrix} \quad (2.4)$$

Наступний заявлений компонент математичної моделі методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри – матриця фіксації санкціонованих (дозволених) дій користувачів $\text{Subject}_i \in \text{SUBJECTS}$ корпоративної мережі в полі інформаційних ресурсів $\text{Object}_j \in \text{OBJECTS}$, яку в моделі ідентифікуємо як матрицю санкціонованих дій MatrixOfAuthorizedActions з узагальненим представленням:

$$\text{MatrixOfAuthorizedActions} = \begin{vmatrix} AA_{1,1} & AA_{1,2} & \cdots & AA_{1,|\text{OBJECTS}|} \\ AA_{2,1} & AA_{2,2} & \cdots & AA_{2,|\text{OBJECTS}|} \\ \vdots & \vdots & & \vdots \\ AA_{|\text{SUBJECTS}|,1} & AA_{|\text{SUBJECTS}|,2} & \cdots & AA_{|\text{SUBJECTS}|,|\text{OBJECTS}|} \end{vmatrix} \quad (2.5)$$

Кожен елемент матриці санкціонованих дій $AA_{ij} \in \text{MatrixOfAuthorizedActions}$ фактично, буде відігравати роль лічильника санкціонованих дій користувачів $\text{Subject}_i \in \text{SUBJECTS}$ корпоративної мережі в полі інформаційних ресурсів $\text{Object}_j \in \text{OBJECTS}$, які не порушують прав доступу користувачів до інформаційних ресурсів мережі. В даній інтерпретації математичної моделі як лічильники накопичення будуть працювати лише елементи $AA_{ij} \in \text{MatrixOfAuthorizedActions}$, для яких $AR_{ij}=1$ ($AR_{ij} \in \text{MatrixOfAccessRights}$), тобто, робота користувача з ресурсами, до яких йому надано права доступу.

І останній із заявлених матричних компонент математичної моделі методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри – матриця фіксації спроб (вдалих або невдалих, несанкціонованого доступу тощо) здійснення несанкціонованих (заборонених) дій користувачів $\text{Subject}_i \in \text{SUBJECTS}$ корпоративної мережі в полі інформаційних ресурсів $\text{Object}_j \in \text{OBJECTS}$, яку в моделі ідентифікуємо як матрицю заборонених дій MatrixOfProhibitedActions з узагальненим представленням:

$$\text{MatrixOfProhibitedActions} = \begin{vmatrix} PA_{1,1} & PA_{1,2} & \cdots & PA_{1,|\text{OBJECTS}|} \\ PA_{2,1} & PA_{2,2} & \cdots & PA_{2,|\text{OBJECTS}|} \\ \vdots & \vdots & & \vdots \\ PA_{|\text{SUBJECTS}|,1} & PA_{|\text{SUBJECTS}|,2} & \cdots & PA_{|\text{SUBJECTS}|,|\text{OBJECTS}|} \end{vmatrix} \quad (2.6)$$

Кожен елемент матриці заборонених дій $PA_{ij} \in$MatrixOfProhibitedActions фактично, буде відігравати роль лічильника спроб (вдалих або невдалих) несанкціонованого доступу користувача $\text{Subject}_i \in$SUBJECTS до інформаційного ресурсу $\text{Object}_j \in$OBJECTS корпоративної мережі, які порушують надані відповідному користувачу права доступу до інформаційних ресурсів мережі. В даній інтерпретації математичної моделі як лічильники накопичення заборонених дій будуть працювати елементи $PA_{ij} \in$MatrixOfProhibitedActions, для яких $AR_{ij}=0$ ($AR_{ij} \in$MatrixOfAccessRights), тобто, дії користувача з ресурсами, до яких йому заборонено доступ.

Матриці санкціонованих дій MatrixOfAuthorizedActions і заборонених дій MatrixOfProhibitedActions відображають задекларовану в концептуальних положеннях приналежність математичної моделі методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри до різновидів статистичних моделей, оскільки вони мають використовуватись для аналізу випадкових процесів та подій у корпоративній мережі, пов’язаних з непередбачуваною поведінкою користувачів $\text{Subject}_i \in$SUBJECTS цієї мережі, яку апріорно не можна передбачити.

Наступним кроком деталізуємо в математичній моделі задекларовану в концептуальних її положеннях ймовірнісну статистичну складову, якою передбачається використання ймовірнісні підходів прогнозування-попередження зловмисних дій та статистичних методів аналізу поведінки користувачів.

Статистичний аналіз поведінки користувачів передбачається здійснювати за даними матриці санкціонованих дій MatrixOfAuthorizedActions і матриці заборонених дій MatrixOfProhibitedActions через зведення статистичних даних до оцінок статистичної імовірності діяльності без порушень положень політики безпеки користувачами корпоративної мережі $\text{Subject}_i \in$SUBJECTS. Перехід від статистичних даних до імовірнісних оцінок будемо виконувати традиційними для таких задач способами через розрахунок $\text{Subject}_i \in$SUBJECTS співвідношення

несанкціонованих дій кожного користувача $\text{Subject}_i \in \text{SUBJECTS}$ до його загальної активності:

$$P(\text{AuthorizedActions})_i = \sum_{\forall(AA_{ij}+PA_{ij})>0}^{|OBJECTS|}{}_{j=0} \frac{AA_{ij}}{AA_{ij}+PA_{ij}}, \qquad (2.7)$$

де $P(\text{AuthorizedActions})_i$ – статистична імовірність роботи без несанкціонованих дій користувача $\text{Subject}_i \in \text{SUBJECTS}$ в полі OBJECTS інформаційних ресурсів корпоративної мережі. Обмеження $\forall(AA_{ij}+PA_{ij})>0$ в формулу (2.7) введене через можливу нульову статистичну активність користувачів, які з різних причин ще не працювали в мережі (новозарахованих користувачів тощо), яку слід враховувати при обчисленні статистичної імовірності санкціонованих дій $P(\text{AuthorizedActions})_i$ для уникнення ситуації з діленням на нуль.

Фактично, статистична імовірність несанкціонованих дій користувача $\text{Subject}_i \in \text{SUBJECTS}$ в полі OBJECTS інформаційних ресурсів корпоративної мережі і передбачається до використання як основний критерій довіри методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри.

Таким чином, введення до математичної моделі методу показника статистичної імовірності роботи без несанкціонованих дій $P(\text{AuthorizedActions})_i$ як критерія довіри забезпечує задекларовану в концептуальних положеннях приналежність математичної моделі методу захисту інформаційних ресурсів корпоративної мережі до категорії моделей інформаційної безпеки на концепції довіри, що і слідувало з визначеної у назві методу методології захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу саме на основі імовірнісних оцінок критеріїв довіри.

Отже, математична модель методу базується на аналізі взаємодії між різними суб'єктами (користувачами) та об'єктами (інформаційними ресурсами) в

інформаційному середовищі корпоративної мережі та дозволяє визначати ступінь довіри до суб'єктів з точки зору інформаційної безпеки.

Для більш наочного представлення імовірнісних критеріїв довіри введемо в математичну модель методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри векторну форму групування значень критеріїв довіри до користувачів $\forall(AA_{ij} + PA_{ij}) > 0$ у вигляді вектора критеріїв довіри VectorOfTrustCriteria:

$$\text{VectorOfTrustCriteria} = \begin{vmatrix} P(\text{AuthorizedActions})_1 \\ P(\text{AuthorizedActions})_2 \\ \vdots \\ P(\text{AuthorizedActions})_{|\text{SUBJECTS}|} \end{vmatrix}. \qquad (2.8)$$

Для забезпечення можливості автоматизованого керування доступом до інформаційних ресурсів корпоративної мережі на основі імовірнісних оцінок критеріїв довіри передбачимо в математичній моделі граничні обмеження блокування прав доступу користувачів $\text{Subject}_i \in \text{SUBJECTS}$ за критерієм довіри до кожного облікованого інформаційного ресурсу $\text{Object}_j \in \text{OBJECTS}$, які також згрупуємо у вектор граничних обмежень VectorOfBoundaryConstraints:

$$\text{VectorOfBoundaryConstraints} = \begin{vmatrix} BC_1 \\ BC_2 \\ \vdots \\ BC_{|\text{OBJECTS}|} \end{vmatrix}, \qquad (2.9)$$

де BC_j – рівень обмеження довірчого допуску до ресурсу $\text{Object}_j \in \text{OBJECTS}$, який розглядається як гранична нижня межа значення імовірнісної оцінки довіри $P(\text{AuthorizedActions})_i$ до користувача $\text{Subject}_i \in \text{SUBJECTS}$, після зменшення довіри нижче якої ($P(\text{AuthorizedActions})_i < BC_j$) доступ до ресурсу

$Object_j \in OBJECTS$ користувачу $Subject_i \in SUBJECTS$ автоматично блокується до прийняття рішення щодо подальших заходів комісією (експертами) з розслідування інцидентів інформаційної безпеки.

2.3 Висновки

В другому розділі запропоновано математичну модель методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри.

В ході розробки математичної моделі методу першочергово здійснено визначення її типу і загальних концептуальних положень.

За результатами аналізу покладених на метод завдань, концептуально математичну модель методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри класифіковано як ймовірнісну статистичну модель систем управління доступом на основі концепції (критеріїв) довіри.

Математична модель методу базується на аналізі взаємодії між різними суб'єктами (користувачами) та об'єктами (інформаційними ресурсами) в інформаційному середовищі корпоративної мережі та дає інструментарій для визначення ступеня довіри до суб'єктів інформаційних відносин в корпоративній мережі з точки зору інформаційної безпеки.

При створенні математичної моделі методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри використані положення теорії множин, теорії матриць, математичної статистики та теорії ймовірностей, булевої алгебри, концепції довіри інформаційної безпеки тощо.

3 РОЗРОБКА МЕТОДУ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ КОРПОРАТИВНОЇ МЕРЕЖІ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ НА ОСНОВІ ІМОВІРНІСНИХ ОЦІНОК КРИТЕРІЇВ ДОВІРИ

3.1 Концепція методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри

Перед безпосередньою розробкою будь-якого методу першочергово необхідно визначитись з його концепцією.

Першочергово при формулюванні концепції методу слід визначити мету або призначення методу, тобто, визначитись, чого саме планується досягти або вирішити за допомогою даного методу.

Мета кваліфікаційної роботи полягає у підвищенні ефективності захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу за рахунок реалізації контролю поведінки користувачів і корекції їх прав доступу в реальному масштабі часу на основі імовірнісних оцінок критеріїв довіри.

Відповідно до мети кваліфікаційної роботи, призначення (мета тощо) самого методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри полягає у підвищенні ефективності захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу.

Призначення методу захисту інформаційних ресурсів корпоративної мережі визначає загальний напрямок досліджень і є основою для уточнення завдань методу, реалізовуваних для досягнення мети, принципів і підходів щодо виконання цих завдань, тобто, призначення методу визначає основні правила та ідеї, на яких ґрунтується метод.

Стосовно методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри основні його ідеї та принципи наступні:

– метод розробляється для підвищення ефективності захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу;

– метод базується на виявленні аномальної поведінки користувачів інформаційних ресурсів корпоративної мережі і обмеженні прав доступу до зазначених ресурсів при виявленні порушень користувачем вимог політики безпеки роботи в мережі;

– реагування на порушення користувачем вимог політики безпеки роботи в корпоративній мережі з прийняттям рішення щодо обмеження доступу до її інформаційних ресурсів має здійснюватися системою захисту інформації автоматично в реальному масштабі часу;

– реалізація методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри в реальному масштабі часу системою захисту без втручання людини зумовлює потребу у використанні читко визначеного математичного базису та правил роботи методу на основі цього базису, що є основою для алгоритмічної і подальшої технічної (програмної) реалізації методу;

– математичною основою методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри є визначена і описана в попередньому розділі пояснювальної записки ймовірнісна статистична математична модель управління доступом на основі концепції (критеріїв) довіри;

– базовим критерієм для динамічного управління розподілом прав доступу є імовірнісний критерій довіри, що розраховується і постійно динамічно корегується з урахуванням активності користувача в мережі;

– імовірнісний критерій довіри до користувача є основним при визначенні і зміні прав користувача на доступ до інформаційних ресурсів корпоративної

мережі та при автоматичному блокуванні доступу користувача до зазначених ресурсів тощо.

Методики, прийоми та засоби, які використовуються для збору статистичних даних щодо поведінки користувачів, їх аналізу і обробки, алгоритми виконання конкретних завдань у рамках методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри базуються на ймовірнісній статистичній математичній моделі управління доступом на основі концепції (критеріїв) довіри, тому доцільним є більш детальний аналіз особливостей реалізації концепції пропонованого методу в термінах математичної моделі.

3.2 Реалізація концепції методу в термінах математичної моделі

Запропонована в попередньому розділі пояснювальної записки математична модель методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри є його основою і містить необхідний інструментарій для його реалізації, що потребує детального аналізу особливостей реалізації концепції пропонованого методу в термінах математичної моделі.

Метод базується на аналізі характеру дій (активностей) користувачів інформаційних ресурсів, що в математичній моделі розглядається як взаємодія зазначених суб’єктів і об’єктів інформаційних відносин, відображених в моделі множинами SUBJECTS (2.1) і OBJECTS (2.2) відповідно.

Базовим елементом визначення прав доступу користувачів $Subject_i \in SUBJECTS$ до інформаційних ресурсів $Object_j \in OBJECTS$ корпоративної мережі є бінарна матриця прав доступу MatrixOfAccessRights (2.4) булевого типу, яка заповнюється за правилами, визначеними системою залежностей (2.3).

Базовим критерієм для динамічного управління розподілом прав доступу є імовірнісний критерій довіри $P(\text{AuthorizedActions})_i$, що розраховується і постійно динамічно корегується з урахуванням активності користувача $\text{Subject}_i \in \text{SUBJECTS}$ в мережі, яка зводиться до статистики дій користувача корпоративної мережі.

Накопичувані статистичні дані щодо дій суб'єктів $\text{Subject}_i \in \text{SUBJECTS}$ інформаційних відносин над об'єктами $\text{Object}_j \in \text{OBJECTS}$ корпоративної мережі формуються з розподілом даних щодо дій користувачів на коректні і некоректні з точки зору дотримання вимог політики безпеки роботи в мережі та узагальнюються в моделі у формі матриць санкціонованих дій MatrixOfAuthorizedActions (2.5) і матрицю заборонених дій MatrixOfProhibitedActions (2.6) .

Імовірнісний критерій довіри розраховується на основі накопичуваних статистичних даних щодо дій суб'єктів інформаційних відносин над об'єктами (інформаційними ресурсами) корпоративної мережі (даних матриці санкціонованих дій MatrixOfAuthorizedActions (2.5) і матриці заборонених дій MatrixOfProhibitedActions (2.6)) за формулою (2.7) і узагальнюється для всіх користувачів $\text{Subject}_i \in \text{SUBJECTS}$ інформаційних ресурсів корпоративної мережі в формі у вигляді вектора критеріїв довіри VectorOfTrustCriteria (2.8).

Вектор критеріїв довіри VectorOfTrustCriteria до користувачів $\text{Subject}_i \in \text{SUBJECTS}$ інформаційних ресурсів корпоративної мережі, який, фактично, є відображенням статистичної імовірності несанкціонованих дій користувача $\text{Subject}_i \in \text{SUBJECTS}$ в полі OBJECTS інформаційних ресурсів корпоративної мережі, передбачається до використання як основний критерій довіри методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри і як інструмент динамічного управління правами доступу користувачів до ресурсів корпоративної мережі.

Для реалізації динамічного управління правами доступу користувачів $Subject_i \in SUBJECTS$ до ресурсів $Object_j \in OBJECTS$ корпоративної мережі використовуються рівні обмеження довірчого допуску до кожного інформаційного ресурсу $Object_j \in OBJECTS$, систематизовані у вигляді вектора граничних обмежень VectorOfBoundaryConstraints (2.9) довірчого допуску до ресурсів корпоративної мережі.

Якщо відображувана вектором критеріїв довіри VectorOfTrustCriteria статистика дій певного користувача $Subject_i \in SUBJECTS$ в полі OBJECTS інформаційних ресурсів корпоративної мережі призводить до падіння рівня його довіри нижче за обмеження довірчого допуску до певного інформаційного ресурсу $Object_j \in OBJECTS$ корпоративної мережі, то доступ відповідного користувача до цього ресурсу блокується.

Структурно-логічна схема концепції методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри в термінах математичної моделі представлена на рисунку 3.1.

Блокування доступу користувача $Subject_i \in SUBJECTS$ до інформаційного ресурсу $Object_j \in OBJECTS$ передбачає зміну статусу зазначеного в матриці прав доступу MatrixOfAccessRights рівня прав доступу користувача – зміну значення елемента $AR_{ij} \in$ MatrixOfAccessRights на нульове. Умова $AR_{ij}=0$, відповідно, блокує доступ користувача $Subject_i \in SUBJECTS$ до інформаційного ресурсу $Object_j \in OBJECTS$ відповідно до раніше визначених положень математичної моделі методу.

На рисунку 3.2 представлена схема причинно-наслідкових зв’язків між елементами математичної моделі в концепції реалізації методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри.

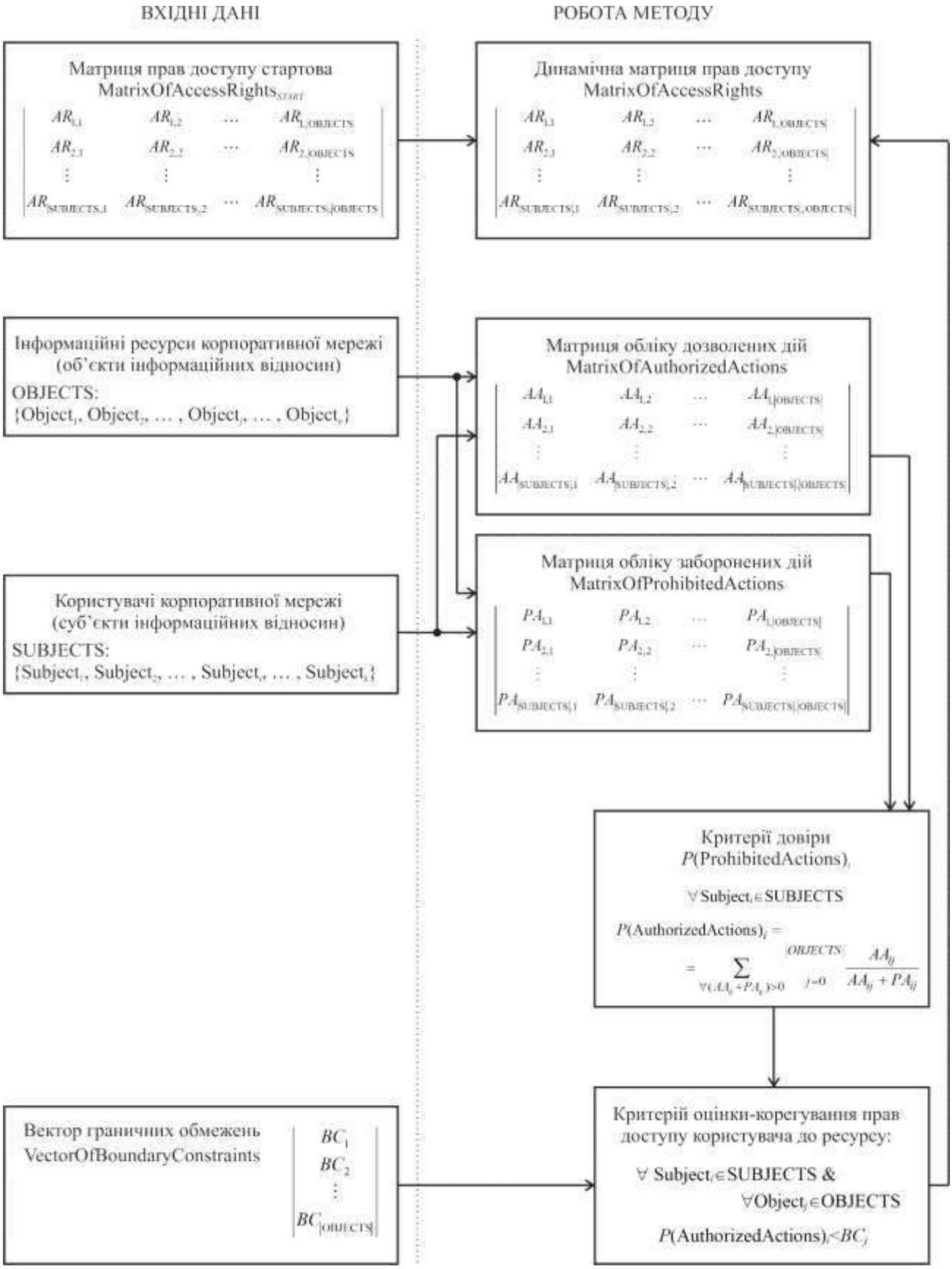


Рисунок 3.1 – Структурно-логічна схема концепції методу в термінах математичної моделі

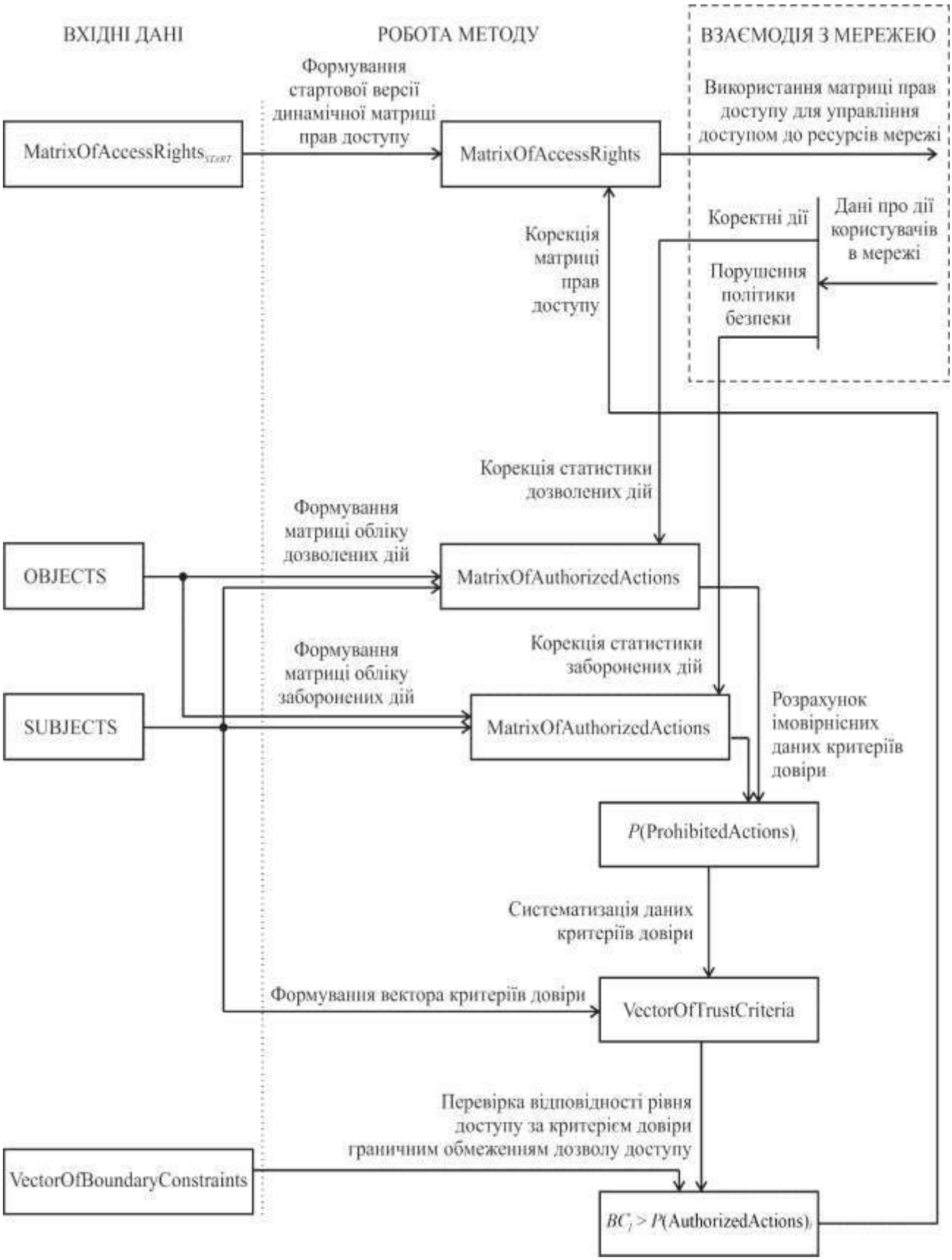


Рисунок 3.2 – Причинно-наслідкова схема реалізації концепції методу в термінах математичної моделі

Схема причинно-наслідкових зв’язків містить всі елементи математичної моделі, які були відображені на структурно-логічній схемі концепції методу в термінах математичної моделі (рисунок 3.1), але без їх деталізації. В той же час, на схемі причинно-наслідкових зв’язків поряд із лініями зв’язків деталізовано характер змін даних математичної моделі при переході від одного її елемента до іншого. Також на схемі причинно-наслідкових зв’язків продемонстровано зв’язки методу з роботою самої корпоративної мережі через використання матриці прав доступу для управління доступом до ресурсів мережі (використання результатів роботи методу для управління доступом до інформаційних ресурсів корпоративної мережі на основі критеріїв довіри) та через зворотне отримання від мережі даних про дії користувачів (використання для реалізації методу даних корпоративної мережі щодо статистики дій користувачів з її інформаційними ресурсами), які на вході в схему реалізації методу поділяються на коректні дії з інформаційними ресурсами та дії, які підпадають під категорію порушень політики безпеки роботи в мережі (заборонені для відповідного користувача дії).

3.3 Алгоритмічна реалізація методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри

Алгоритмічну реалізацію методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри будемо здійснювати на основі вже визначеної в цій роботі концепції методу та з урахуванням принципів реалізації концепції методу в термінах математичної моделі, що представлені у формі структурно-логічної схеми концепції методу в термінах математичної моделі (рисунок 3.1) і причинно-наслідкової схеми реалізації концепції методу в термінах математичної моделі (рисунок 3.2).

Аналіз причинно-наслідкової схеми реалізації концепції методу в термінах математичної моделі дозволяє виділити три основних фази роботи методу:

– підготовка вхідних даних;

– робота методу (реалізація інноваційної складової методу);

– взаємодія з мережею (використання результатів роботи методу для керування доступом до інформаційних ресурсів мережі та збір статистичних даних для наступних ітерацій реалізації методу).

Уточнення особливостей цих фаз з ціллю їх алгоритмічної реалізації дозволяє визначити основні етапи реалізації методу:

– підготовка вхідних даних;

– формування початкових представлень векторно-матричних складових реалізації методу;

– застосування матриці прав доступу MatrixOfAccessRights для управління доступом до інформаційних ресурсів корпоративної мережі;

– фіксація активності (дій) користувачів інформаційних ресурсів корпоративної мережі;

– класифікація зафіксованих дій користувачів інформаційних ресурсів корпоративної мережі на коректні та на дії з порушенням вимог політики безпеки;

– корекція матриць статистичних даних;

– корекція даних показників критеріїв довіри користувачів;

– корекція матриці прав доступу MatrixOfAccessRights;

– перехід до повторної реалізації циклу починаючи з етапу застосування матриці прав доступу MatrixOfAccessRights.

Зведемо наведений опис основних етапів реалізації методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри до чіткої алгоритмічної послідовності дій.

Алгоритм 3.1. Узагальнений алгоритм реалізації методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри.

3.1.1 Підготовити вхідні дані для реалізації методу.

3.1.2 Сформувати базові представлення векторно-матричних складових реалізації методу.

3.1.3 Надати матрицю прав доступу MatrixOfAccessRights для управління доступом до інформаційних ресурсів корпоративної мережі.

3.1.4 Перевірити дії користувачів інформаційних ресурсів корпоративної мережі.

3.1.5 Якщо нових дій користувачів інформаційних ресурсів не зафіксовано, перейти до п.3.1.4.

3.1.6 Класифікація зафіксованих дій користувачів інформаційних ресурсів корпоративної мережі на коректні та порушення вимог політики безпеки роботи в мережі.

3.1.7 Корекція матриць статистичних даних;

3.1.8 Корекція даних показників критеріїв довіри користувачів;

3.1.9 Корекція матриці прав доступу MatrixOfAccessRights;

3.1.10 Якщо роботу системи завершено, перейти до п.3.1.12.

3.1.11 Перейти до п.3.1.3.

3.1.12 Кінець алгоритму.

На рисунку 3.3 представлена блок-схема узагальненого алгоритму реалізації методу.

Перейдемо до деталізації заявлених етапів узагальненого алгоритму реалізації методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри з метою отримання деталізованого алгоритму реалізації методу.

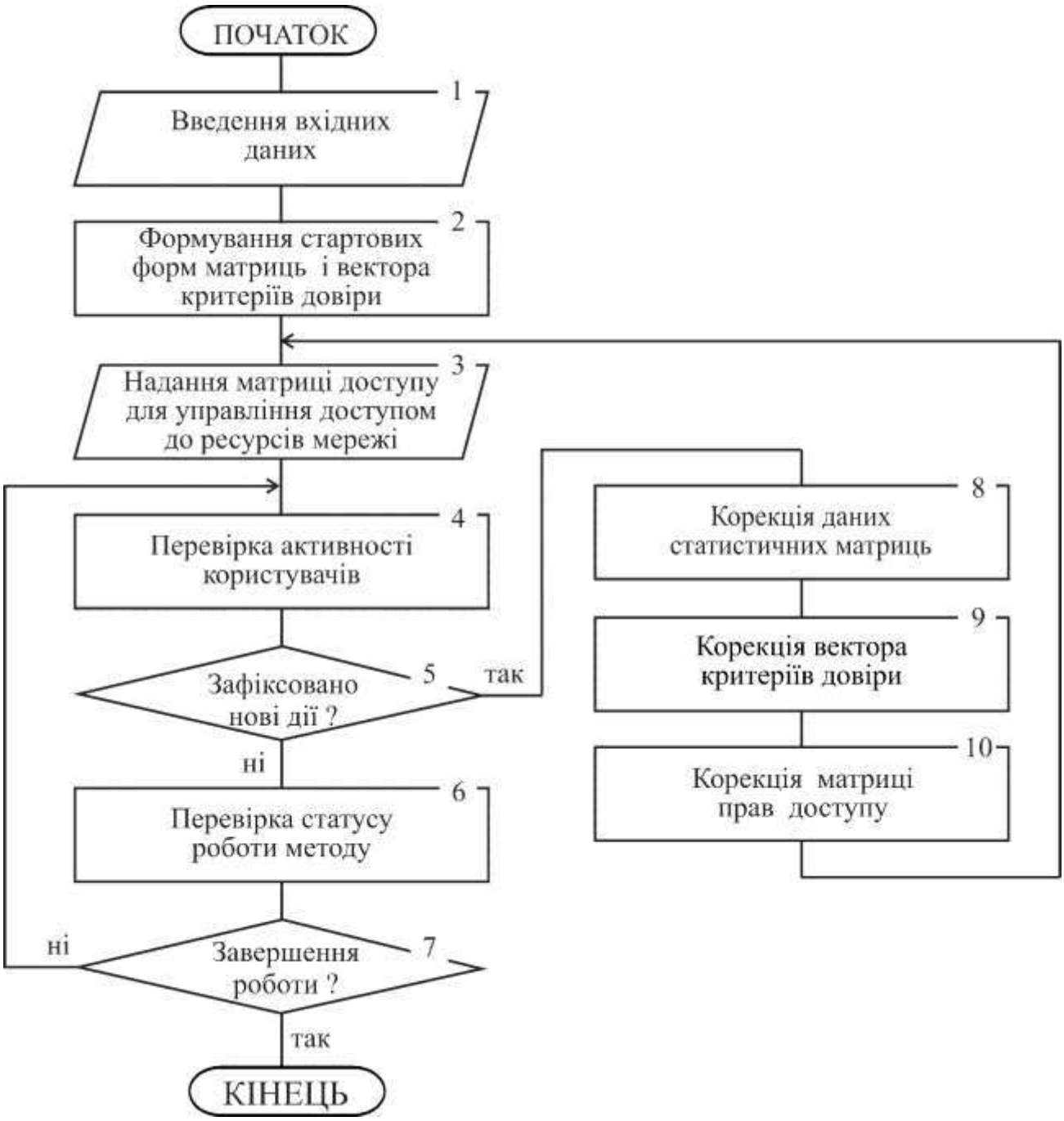


Рисунок 3.3 – Блок-схема узагальненого алгоритму реалізації методу

Етап підготовки вхідних даних методу, як це видно з структурно-логічної схеми концепції методу в термінах математичної моделі і причинно-наслідкової схеми реалізації концепції методу в термінах математичної моделі, передбачає формування чотирьох базових компонентів моделі методу:

– множина ідентифікаторів всіх користувачів корпоративної мережі SUBJECTS;

– множина ідентифікації облікованих в реалізації методу інформаційних ресурсів корпоративної мережі OBJECTS;

– стартовий варіант матриці прав доступу MatrixOfAccessRights;

– вектор граничних обмежень VectorOfBoundaryConstraints.

Зазначені компоненти є вхідними даними для реалізації методу і потребують визначення до його практичного застосування.

Практичне застосування (робота) методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри починається з визначення стартового варіанту матриці прав доступу MatrixOfAccessRights в якості робочого, який підлягає подальшій модифікації в процесі реалізації методу. Робочий варіант матриці прав доступу MatrixOfAccessRights застосовується як інструмент для управління доступом до інформаційних ресурсів корпоративної мережі зі старту роботи методу (тобто, саме на старті роботи методу для управління доступом до інформаційних ресурсів корпоративної мережі використовується стартовий варіант матриці прав доступу MatrixOfAccessRights як робочий).

Застосування матриці прав доступу MatrixOfAccessRights для управління доступом до інформаційних ресурсів корпоративної мережі полягає в наданні або блокуванні доступу користувачам $Subject_i \in SUBJECTS$ до кожного облікованого інформаційного ресурсу $Object_j \in OBJECTS$.

При наданні доступу користувачам $Subject_i \in SUBJECTS$ до ресурсів $Object_j \in OBJECTS$ мережі здійснюється контроль за роботою користувачів та класифікація їх дій. Кожна спроба здійснення доступу фіксується і обробляється. Обробка полягає у визначенні, чи здійснено доступ у відповідності до вимог політики безпеки роботи з ресурсами мережі, або ж з порушенням цих вимог. Залежно від результатів аналізу коректності дій їх класифікують на дозволені і заборонені.

Описана процедура контролю за роботою та класифікації дій користувачів передбачає наступні етапи:

– фіксація наявності дій користувача інформаційних ресурсів корпоративної мережі;

– ідентифікація користувача $Subject_i \in SUBJECTS$, активність якого зафіксовано;

– ідентифікація ресурсу мережі $Object_j \in OBJECTS$, до якого здійснюється доступ користувача $Subject_i \in SUBJECTS$;

– аналіз коректності дій користувача $Subject_i \in SUBJECTS$ та їх класифікація на дозволені чи заборонені (порушення вимог політики безпеки роботи в мережі).

Після ідентифікації і класифікації зафіксованих дій користувача $Subject_i \in SUBJECTS$ в полі інформаційних ресурсів мережі OBJECTS метод захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри переходить до етапу корекції статистичних даних щодо дій користувача в мережі та перерахунку рівня довіри до користувача за відповідним критерієм:

– якщо дії користувача $Subject_i \in SUBJECTS$ стосовно ресурсу $Object_j \in OBJECTS$ класифіковано як дозволені, здійснюється корекція матриці санкціонованих дій MatrixOfAuthorizedActions через інкремент значення коректних дій користувача з ресурсом $AA_{ij} \in$ MatrixOfAuthorizedActions;

– якщо дії користувача $Subject_i \in SUBJECTS$ стосовно ресурсу $Object_j \in OBJECTS$ класифіковано як заборонені (порушення вимог політики безпеки роботи в мережі) – здійснюється корекція матриці заборонених дій MatrixOfProhibitedActions через інкремент $PA_{ij} \in$ MatrixOfProhibitedActions зафіксованих заборонених дій користувача з ресурсом;

– перерахунок імовірнісного показника рівня довіри $P(\text{AuthorizedActions})_i$ до користувача $Subject_i \in SUBJECTS$ за відповідним критерієм за формулою (2.7);

– корекція вектора критеріїв довіри VectorOfTrustCriteria в значенні $P(\text{AuthorizedActions})_i \in$ VectorOfTrustCriteria.

Після корекції статистичних даних щодо дій користувача в мережі та перерахунку рівня довіри до користувача за відповідним критерієм метод захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри переходить до етапу корекції рівня доступу зазначеного користувача $\text{Subject}_i \in \text{SUBJECTS}$. Фактично, корекція рівня доступу користувача $\text{Subject}_i \in \text{SUBJECTS}$ потрібна лише у випадку зниження показника довіри до нього відносно попередньо зафіксованого, тому процедуру корекції можна описати наступним чином:

– перевірка змін імовірнісного показника довіри $P(\text{AuthorizedActions})_i$ до користувача $\text{Subject}_i \in \text{SUBJECTS}$ (якщо рівень довіри не зменшено, наступні корки не виконуються);

– порівняння імовірнісного показника довіри $P(\text{AuthorizedActions})_i$ до користувача $\text{Subject}_i \in \text{SUBJECTS}$ з гранично допустимим рівнем імовірнісної довіри для доступу до кожного ресурсу $\text{Object}_j \in \text{OBJECTS}$, представленого значенням граничної нижня межа BC_j у векторі граничних обмежень VectorOfBoundaryConstraints;

– перевірка-корекція рівня доступу користувача $\text{Subject}_i \in \text{SUBJECTS}$ до ресурсів $\text{Object}_j \in \text{OBJECTS}$ у матриці прав доступу MatrixOfAccessRights: якщо для певного ресурсу у користувача наявний доступ, що зафіксовано значенням $AR_{ij}=1$ ($AR_{ij} \in \text{MatrixOfAccessRights}$), і при порівнянні визначається зниження імовірнісного показника довіри $P(\text{AuthorizedActions})_i$ до користувача нижче гранично-допустимого значення $BC_j \in \text{VectorOfBoundaryConstraints}$ для доступу до ресурсу $\text{Object}_j \in \text{OBJECTS}$, то доступ до відповідного ресурсу користувачу блокується фіксацією значення $AR_{ij}=0$ ($AR_{ij} \in \text{MatrixOfAccessRights}$).

Після цього відбувається перехід до повторної реалізації циклу починаючи з етапу застосування матриці прав доступу MatrixOfAccessRights для управління доступом до інформаційних ресурсів корпоративної мережі.

Зведемо наведений деталізований опис основних етапів реалізації методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого

доступу на основі імовірнісних оцінок критеріїв довіри до алгоритмічної послідовності дій.

Алгоритм 3.2. Деталізований алгоритм реалізації методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри.

3.2.1 Визначити склад множини OBJECTS.

3.2.2 Визначити склад множини SUBJECTS.

3.2.3 Визначити стартові права доступу у вигляді матриці прав доступу MatrixOfAccessRights.

3.2.4 Задати граничні обмеження блокування прав доступу до ресурсів мережі як вектор граничних обмежень VectorOfBoundaryConstraints.

3.2.5 Надати матрицю прав доступу MatrixOfAccessRights для управління доступом до інформаційних ресурсів корпоративної мережі.

3.2.6 Перевірити наявність дії користувачів інформаційних ресурсів корпоративної мережі.

3.2.7 Якщо дій користувачів інформаційних ресурсів не зафіксовано, перейти до п.3.2.6.

3.2.8 Ідентифікувати користувача $Subject_i \in SUBJECTS$, активність якого зафіксовано.

3.2.9 Ідентифікувати ресурс мережі $Object_j \in OBJECTS$, до якого здійснюється доступ користувача $Subject_i \in SUBJECTS$;

3.2.10 Аналіз прав доступу користувача $Subject_i \in SUBJECTS$ до ресурсу $Object_j \in OBJECTS$: якщо $AR_{ij}=1$, перейти до п.3.2.13.

3.2.11 Корекція матриці санкціонованих дій MatrixOfAuthorizedActions: $AA_{ij}=AA_{ij}+1$;

3.2.12 Перейти до п.3.2.21.

3.2.13 Корекція матриці заборонених дій MatrixOfProhibitedActions: $PA_{ij}=PA_{ij}+1$;

3.2.14 Тимчасове зберігання поточного значення рівня ймовірнісного критерія довіри користувача $TMP=P(\text{AuthorizedActions})_i$;

3.2.15 Перерахунок імовірнісного показника рівня довіри $P(\text{AuthorizedActions})_i$ за формулою (2.7) (корекція вектора критеріїв довіри VectorOfTrustCriteria в значенні $P(\text{AuthorizedActions})_i \in \text{VectorOfTrustCriteria}$).

3.2.16 Перевірка факту зниження імовірнісного показника рівня довіри до користувача: якщо $TMP\text{-}P(\text{AuthorizedActions})_i \leq 0$, перейти до п. 3.2.21.

3.2.17 $j=1$ – ініціалізація лічильника для перевірки-корекції рівня доступу користувача $\text{Subject}_i \in \text{SUBJECTS}$ до ресурсів $\text{Object}_j \in \text{OBJECTS}$ у матриці прав доступу MatrixOfAccessRights;

3.2.18 Якщо $AR_{ij}=1$ і $P(\text{AuthorizedActions})_i < BC_j$, то прийняти $AR_{ij}=0$.

3.2.19 $j=j+1$ – інкремент лічильника (перехід до перевірки-корекції рівня доступу користувача $\text{Subject}_i \in \text{SUBJECTS}$ до наступного ресурсу $\text{Object}_j \in \text{OBJECTS}$).

3.2.20 Якщо $j < \left|\text{OBJECTS}\right|$ (не завершено перевірку-корекцію рівня доступу користувача $\text{Subject}_i \in \text{SUBJECTS}$ до всіх ресурсів $\text{Object}_j \in \text{OBJECTS}$), перейти до п. 3.2.18.

3.2.21 Якщо роботу системи завершено, перейти до п.3.2.23.

3.2.22 Перейти до п.3.2.5.

3.2.23 Кінець алгоритму.

На рисунку 3.4 деталізований алгоритм реалізації методу представлено блок-схемою.

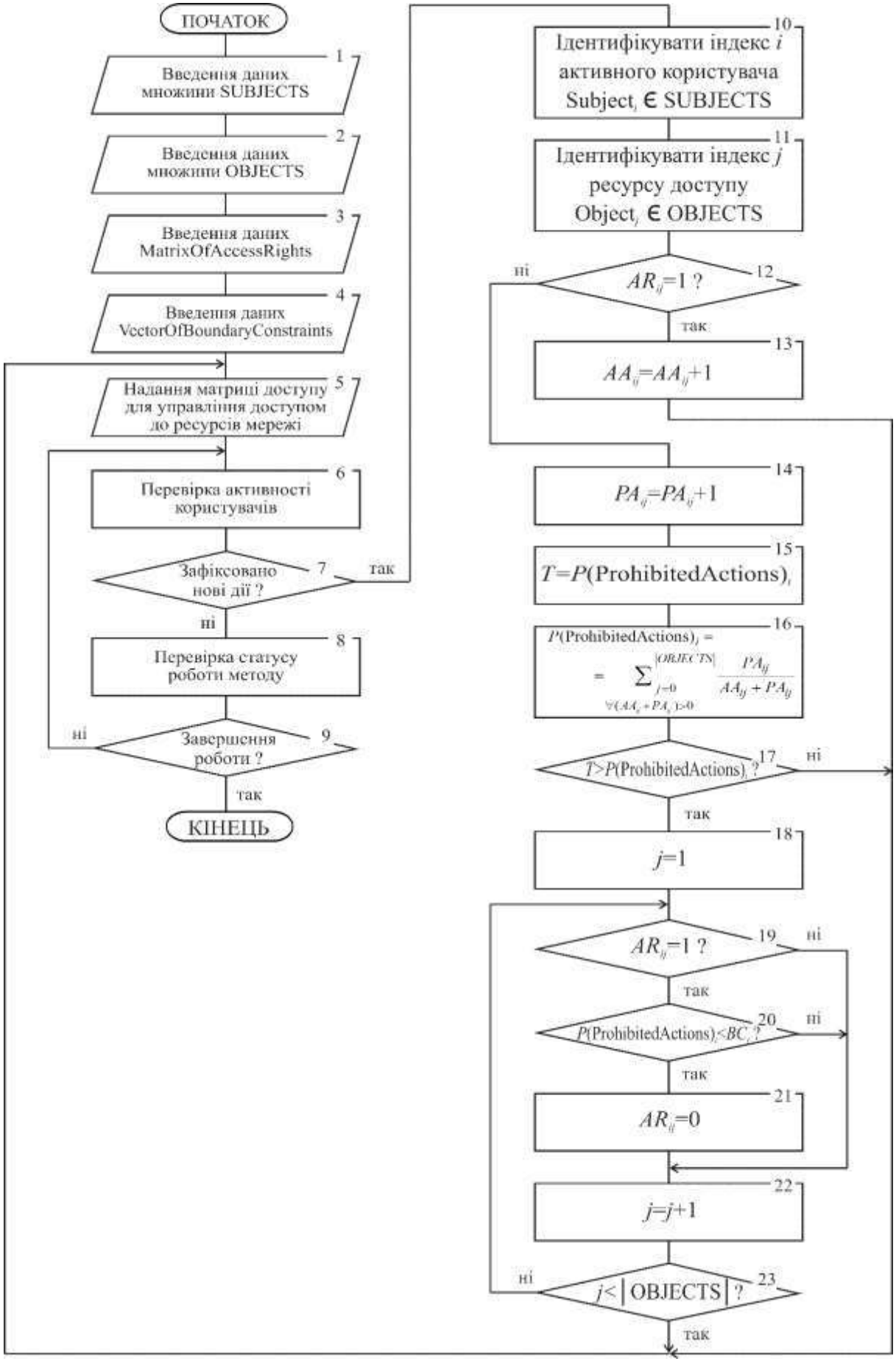


Рисунок 3.4 – Блок-схема деталізованого алгоритму реалізації методу

3.4 Висновки

В третьому розділі роботи презентовано метод захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри.

Першочергово визначено концепцію методу як базову теоретичну основу, яка лягає в основі вирішення проблеми і здійснення передбачуваних методом дій. Запропонована концепція методу, фактично, встановлює загальний курс дій та рекомендації для досягнення поставленої мети методу.

Оскільки прийоми та засоби, які використовуються для збору статистичних даних щодо поведінки користувачів згідно концепції методу, їх аналізу і обробки, алгоритми виконання конкретних завдань у рамках методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри базуються на ймовірнісній статистичній математичній моделі управління доступом, то в розділі здійснено детальний аналіз особливостей реалізації концепції пропонованого методу в термінах математичної моделі, що дозволило синтезувати і представити структурно-логічну схему концепції методу і причинно-наслідкову схему реалізації концепції методу в термінах математичної моделі.

На основі концепції методу та з урахуванням принципів реалізації концепції методу в термінах математичної моделі у формі структурно-логічної схеми і причинно-наслідкової схеми запропоновано алгоритмічну реалізацію методу, яка подана в формі узагальненого і деталізованого алгоритму реалізації методу.

4 АПРОБАЦІЯ МЕТОДУ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ КОРПОРАТИВНОЇ МЕРЕЖІ

4.1 Дослідження актуальних загроз безпеці інформаційних ресурсів корпоративної мережі і можливостей методу

Поняття безпеки корпоративних мереж охоплює стан захищеності ресурсів мережі від випадкових чи навмисних втручань у її нормальний функціональний процес, а також від спроб несанкціонованого доступу, модифікації чи фізичного пошкодження її компонентів. Іншими словами, це здатність протистояти різноманітним шкідливим впливам на інформаційну безпеку.

Загрози безпеці інформаційних ресурсів корпоративної мережі включають дії або події, які можуть призвести до несанкціонованого доступу до інформації, її спотворення або навіть до руйнування інформаційних ресурсів корпоративних мереж, а також програмних та апаратних засобів. Це може охоплювати такі загрози, як хакерські атаки, віруси, шпигунське програмне забезпечення, фішинг та інші форми кіберзлочинності, що можуть серйозно підірвати стійкість та надійність мережевої інфраструктури [43].

У сфері корпоративних мереж широко використовується термін вразливість, що означає слабкі місця або недоліки, які дозволяють зловмисникам створити загрозу для системи. Це може включати недостатню захищеність від несанкціонованого доступу, можливість зміни інформації, а також ризик виведення з ладу програмного та апаратного забезпечення [44].

Для здійснення шкідливих дій, таких як несанкціонований доступ, зміна інформації, або навіть відключення програм та апаратного обладнання, зловмисники можуть використовувати атаки на ресурси корпоративних мереж. Атака в цьому контексті – це небажана дія, що виконується зловмисником, спрямована на використання конкретної вразливості в системі.

Зазвичай, у сфері кібербезпеки виділяють три основні види загроз: загрози розкриття, цілісності та відмови в обслуговуванні.

Загроза розкриття передбачає можливість незаконного доступу до конфіденційної інформації для осіб, які не мають на це права. Це може призвести до небажаного витоку чутливих даних, який часто охарактеризовують як виток або крадіжку інформації. У контексті інформаційної безпеки інформаційних ресурсів корпоративної мережі, загроза цілісності даних виникає, коли зловмисники навмисно вносять зміни в інформацію, що зберігається на пристроях корпоративних мереж або передається через канали зв'язку. Зазвичай, загрози цілісності найбільше турбують бізнес-сферу, оскільки вони можуть призвести до серйозних фінансових втрат та порушення ділової репутації.

Загроза відмови в обслуговуванні системи (DDoS-атака) виника в результаті зловживання певними діями, що можуть спричинити блокування доступу до обчислювальних ресурсів. Це може бути тимчасовим блокуванням, коли ресурс стає недоступним на деякий час, або постійним, коли доступ до ресурсу в мережі корпорації повністю відсутній. В останньому випадку мова йде про вичерпання ресурсу, оскільки він стає непридатним для використання протягом тривалого періоду. Це може призвести до серйозних проблем з продуктивністю корпоративних мереж та можливістю виконання бізнес-процесів, що впливає на ефективність організації.

У локальних обчислювальних мережах корпоративного використання найбільш поширеними є загрози цілісності та розкриття інформації, тоді як в глобальному масштабі для мереж потужних багатоофісних корпорацій переважає загроза відмови в обслуговуванні.

До традиційної кібербезпекової моделі будь-якої корпоративної мережі можна стверджувати, що негативні впливи на неї можуть мати як випадковий, так і умисний характер. Випадкові загрози безпеки інформаційних ресурсів вирізняють часто також ненавмисними [46], їх протилежність – загрози умисні.

Джерелами ненавмисних загроз інформаційних ресурсів корпоративної мережі можуть бути випадкові відмови апаратних засобів, дії працівників без

злих намірів, а також випадкові помилки у програмному забезпеченні та інші непередбачувані обставини. Ці загрози також потрібно враховувати, оскільки вони можуть призвести до значних втрат.

Натомість, умисі загрози щодо інформаційних ресурсів корпоративної мережі ґрунтуються на свідомому злочинному намірі, часто з метою отримання конкретної вигоди для зловмисника, який завдає шкоди системі своїми діями. Ці загрози становлять особливий ризик, оскільки можуть бути скеровані на цілеспрямоване підривання стійкості та безпеки корпоративної мережі. Проводячи свої протиправні дії, зловмисники прагнуть знайти джерела конфіденційної інформації, які б надавали їм найбільш достовірну інформацію в максимальному обсязі та при мінімальних витратах на її отримання.

Захист від таких навмисних загроз визнається специфічним змаганням знань та навичок між нападником і захисником інформаційних ресурсів корпоративної мережі[46]. У цьому змаганні перемагає той, хто володіє глибокими знаннями, навичками, досвідом і може передбачити дії опонента.

Саме надання можливості передбачити дії користувача, який відіграє певним чином роль опонента служби захисту, оцінюючи ступінь довіри до нього, є цільовим призначенням методу.

Навмисні загрози інформаційних ресурсів корпоративної мережі також зазвичай поділяють на зовнішні, які виникають ззовні корпорації, та внутрішні, які виникають всередині самої корпорації.

Зовнішні загрози можуть виникати не тільки внаслідок умисних протиправних дій конкурентів або економічного середовища, але й через інші причини, такі як природні катастрофи.

Загалом, метод захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри орієновано на внутрішню мережу корпорації, доступ до ресурсів якої ззовні неможливий або обмежений, але потенційно метод може бути розширений на зовнішні загрози, що не є предметом даної роботи і може розглядатися в подальших дослідженнях як вдосконалення пропонованого методу.

Внутрішні навмисні загрози, що існують всередині корпорації або її мережевої системи, часто визначаються соціальними напругами та складним моральним кліматом, але можуть мати і зловмисний характер з наміром нашкодити корпорації або отримати вигоду поза нею в недоброчесному конкурентному середовищі.

Деталізуємо основні внутрішні загрози для безпеки інформаційних ресурсів корпоративної мережі [43,47-50]:

– несанкціонований доступ до конфіденційної інформації;

– компрометація цілісності інформації;

– несанкціоноване використання ресурсів корпоративних мереж;

– недобросовісне використання ресурсів корпоративних мереж;

– несанкціонований обмін інформацією між користувачами корпоративних мереж;

– порушення інформаційного обслуговування;

– відмова у доступі до інформації корпоративних мереж;

– нелегальне використання привілеїв;

– ненавмисні або помилкові порушення політики безпеки використання інформаційних ресурсів корпоративної мережі;

– неусвідомлені порушення політики безпеки використання інформаційних ресурсів корпоративної мережі (неусвідомлений вихід поза межі власних повноважень або обов’язків);

– порушення політики безпеки використання інформаційних ресурсів корпоративної мережі «з цікавості» (без злого умислу).

Метод захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри орієнтований на виявлення подібних порушень і зменшення ризиків для інформаційних ресурсів в подальшому, але на даному етапі не передбачає аналізу типів порушень і прийняття рішення щодо відновлення довіри до користувача-штрафника. Останнє залишається привілеєм служби інформаційної безпеки

корпорації, яка має слідкувати за випадками порушень, надавати оцінку їх характеру і мотивам порушника та приймати рішення щодо подальших дій в межах службових інструкцій.

При здійсненні певних незаконних дій може мати місце витік конфіденційної інформації. Це поняття включає в себе несанкціонований вихід конфіденційної (секретної) інформації за межі корпоративної мережі або кола осіб, яким ця інформація була доручена в рамках їх службових обов'язків або стала відомою під час роботи. Витік такої інформації може бути наслідком:

– навмисного розголошення конфіденційної інформації;

– несанкціонованого доступу до конфіденційної інформації за допомогою різних технічних каналів;

– навмисних дій, що призводять до незаконного доступу до конфіденційних інформаційних ресурсів корпоративної мережі за різними методами.

Важливо зауважити, що розголошення інформації може бути навмисними діями посадових осіб або користувачів, яким дані відомості були доручені в рамках їх службових обов'язків, або відбуватися через необережність. Це може призвести до того, що інші особи, яким інформація не повинна була стати відомою, отримують до неї доступ.

Для несанкціонованого доступу потрібні значні технічні знання та компетенції. Щодо причин виникнення каналів витоку, часто вони обумовлені конструктивними або технологічними недоліками в схемах корпоративних мереж або експлуатаційним зношуванням складових. Ці недоліки дозволяють зловмисникам створювати пристрої, що працюють на певних фізичних принципах, створюючи при цьому канали передачі інформації, які називають канали витоку.

Незважаючи на те, що витік інформації може бути створений за допомогою спеціальних засобів зацікавленими особами, все ж таки більшість витоків інформації відбувається через елементарні недоробки в системі безпеки і

недбалість співробітників.

Для методу несанкціонований доступ до інформації з ресурсів корпоративних мереж включає в себе незаконне та навмисне здобуття інформації особами, які мають певні права доступу до цих даних.

Методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри спрямований, першочергово, на забезпечення безпеки та ефективного використання інформаційних ресурсів.

Основні завдання методу включають в себе включають:

– аутентифікація користувачів – метод передбачає обов’язкову перевірку ідентичності користувачів, щоб впевнитися, що вони ті, за кого вони видають себе (це може включати в себе введення ідентифікаційних даних, таких як ім'я користувача та пароль, або використання біометричних методів, карток доступу тощо згідно із внутрішньою політикою безпеки корпорації);

– визначення рівня доступу, який має користувач, щоб ідентифікувати визначає, до яких ресурсів (файли, папки, програми) користувач має право отримати доступ, а також які операції він може виконувати з цими ресурсами.

– метод фіксує події доступу, щоб забезпечити можливість аудитування. Статистичні дані подій дозволяють відслідковувати, які користувачі мають доступ до яких ресурсів, і фіксують події, такі як невдачі спроб входу, спроби несанкціонованого доступу тощо для корегування критерія довіри і рівня дступу користувача;

– метод дозволяє адміністраторам ефективно управляти правами доступу користувачів, що включає в себе надання та вилучення прав, визначення ролей користувачів і груп, управління періодом дії прав доступу, а також автоматичне блокування прав доступу за рівнем довіри;

– метод активно захищає мережеві ресурси від несанкціонованого доступу, забороняючи невірно аутентифікованим і неавторизованим користувачам, а

також користувачам з низьким рівнем довіри отримувати доступ до конфіденційної інформації чи системних ресурсів;

– метод включає в себе заходи безпеки для запобігання внутрішнім загрозам, таким як недбалість або навмисні дії в мережі з боку власних співробітників корпорації;

– метод може взаємодіяти з іншими системами безпеки, такими як системи виявлення вторгнень, антивіруси, системи моніторингу мережі, для комплексного захисту корпоративної мережі.

Ці завдання методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри спрямовані на те, щоб забезпечити безпеку інформаційних ресурсів та здійснювати ефективне управління доступом в корпоративній мережі.

4.2 Експериментальна апробація методу

Експериментальна апробація методу має за мету демонстрацію принципів застосування методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри та підтвердження дієвості методу.

Демонстрацію принципів застосування методу здійснимо на основі базових положень методу, схем реалізації концепції методу та алгоритмічних рішень, розроблених в попередньому розділі.

Згідно із узагальненим алгоритмом реалізації методу (алгоритм 3.1) реалізації методу розпочинається з підготовити вхідних даних.

Структурно-логічна схема концепції методу в термінах математичної моделі (рисунок 3.1) ідентифікує вхідні дані як чотири базових компоненти моделі методу (рисунок 4.1).

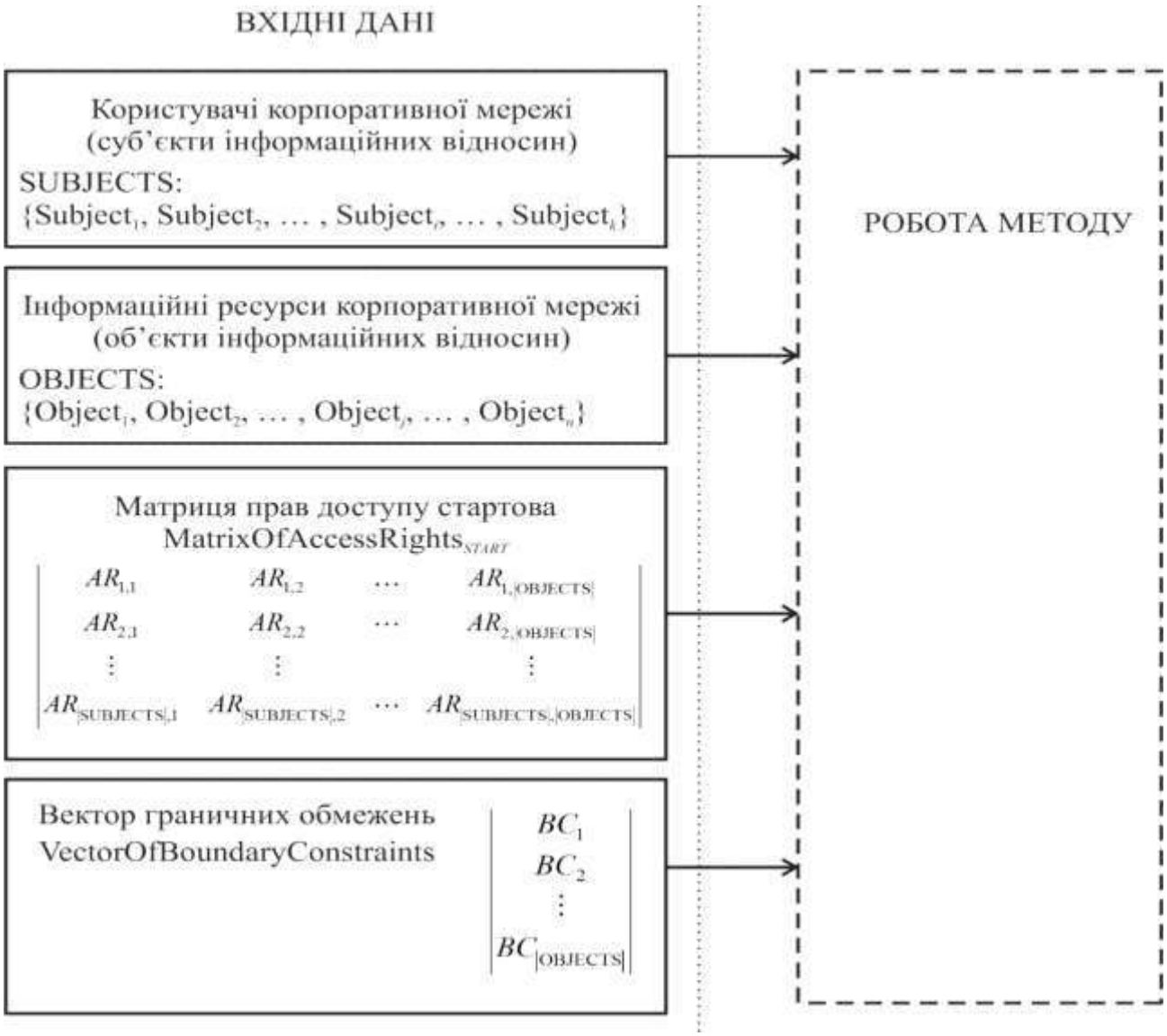


Рисунок 4.1 – Вхідні дані методу

Тобто, етап підготовки вхідних даних методу передбачає формування чотирьох базових компонентів моделі методу:

– множина ідентифікаторів всіх користувачів корпоративної мережі SUBJECTS;

– множина ідентифікації облікованих в реалізації методу інформаційних ресурсів корпоративної мережі OBJECTS;

– стартовий варіант матриці прав доступу MatrixOfAccessRights;

– вектор граничних обмежень VectorOfBoundaryConstraints.

Для експериментальної апробації методу було обрано 10 користувачів корпоративної мережі Хмельницького національного університету, що дало множину SUBJECTS ідентифікаторів користувачів корпоративної мережі $Subject_i \in SUBJECTS$ у вигляді:

$$SUBJECTS:\{Subject_1, Subject_2, Subject_3, Subject_4, \dots, Subject_{10}\}, \quad (4.1)$$

$$\left| SUBJECTS \right| = 10. \quad (4.2)$$

Співставлення ідентифікаторів моделі $Subject_i \in SUBJECTS$ і реальних суб'єктів-користувачів корпоративної мережі відбувається на етапі аутентифікації та ідентифікації цих користувачів.

Одразу зазначимо, що множина SUBJECTS, яка відображує всіх користувачів корпоративної мережі, при реалізації методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри в реальних умовах корпоративної діяльності не є сталою і динамічно змінюється з плином кадрів-користувачів корпоративної мережі.

Також для експериментальної апробації методу було обрано 10 контрольованих ресурсів корпоративної мережі Хмельницького національного університету, що дало множину OBJECTS ідентифікаторів користувачів корпоративної мережі $Object_j \in OBJECTS$ у вигляді:

$$OBJECTS:\{ Object_1, Object_2, Object_3, Object_4, \dots, Object_{10}\}, \quad (4.3)$$

$$\left| OBJECTS \right| = 10. \quad (4.4)$$

Співставлення ідентифікаторів моделі $Object_j \in OBJECTS$ і реальних ресурсів мережі відбувається на етапі формування множини OBJECTS.

Також зазначимо, що множина OBJECTS, яка відображує всіх контрольовані ресурси корпоративної мережі, при реалізації методу в реальних

умовах корпоративної діяльності теж не є сталою і динамічно змінюється зі змінами в організації і інформаційному наповненні корпоративної мережі.

Обмеження (4.4) і формула (2.9) дають нам розмірність і формалізоване представлення вектора граничних обмежень VectorOfBoundaryConstraints під наш експеримент:

$$\text{VectorOfBoundaryConstraints} = \begin{vmatrix} BC_1 \\ BC_2 \\ BC_3 \\ BC_4 \\ BC_5 \\ BC_6 \\ BC_7 \\ BC_8 \\ BC_9 \\ BC_{10} \end{vmatrix}. \quad (4.5)$$

Для реалізації експерименту було прийнято наступні цифрові значення граничних обмежень прав доступу $BC_j \in \text{VectorOfBoundaryConstraints}$:

$$\text{VectorOfBoundaryConstraints} = \begin{vmatrix} 0.96 \\ 0.66 \\ 0.75 \\ 0.89 \\ 0.30 \\ 0.21 \\ 0.98 \\ 0 \\ 0 \\ 0 \end{vmatrix}. \quad (4.6)$$

З вектора (4.6) видно, що ресурси ($Object_8$-$Object_{10}$)$\in$OBJECTS мають нульове граничне обмеження прав доступу ($BC_8=BC_9=BC_{10}=0$), що робить їх загальнодоступними для всіх, кому доступ до відповідного ресурсу не заблоковано в матриці прав доступу MatrixOfAccessRights. Відповідно, знизити рівень довіри нижче нульового порогового значення при реалізації методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри буде неможливо, тому ці ресурси залишаться доступними користувачам $Subject_i\in$SUBJECTS, у яких $AR_{ij}=1$ ($AR_{ij}\in$MatrixOfAccessRights).

Ресурс $Object_7\in$OBJECTS має найжорсткіше граничне обмеження прав доступу ($BC_7=0.98$), що має робити його недоступним для користувачів за відносно невисокого відсотка порушень політики безпеки користування інформаційними ресурсами корпоративної мережі.

Інші значення $BC_j\in$VectorOfBoundaryConstraints градуйовано розподілені з урахуванням ступеня конфіденційності або важливості відповідних їм ресурсів $Object_j\in$OBJECTS.

Обмеження (4.2) і (4.4) та формула (2.4) дають нам розмірність і формалізоване представлення матриці прав доступу MatrixOfAccessRights розмірністю 10 на 10 елементів $AR_{ij}\in$MatrixOfAccessRights:

$$\text{MatrixOfAccessRights} = \begin{vmatrix} AR_{1,1} & AR_{1,2} & \cdots & AR_{1,10} \\ AR_{2,1} & AR_{2,2} & \cdots & AR_{2,10} \\ \vdots & \vdots & & \vdots \\ AR_{10,1} & AR_{10,2} & \cdots & AR_{10,10} \end{vmatrix} \qquad (4.7)$$

Для реалізації експерименту, з урахуванням визначених системою (2.3) правил, було прийнято наступні бінарні значення прав доступу $AR_{ij}\in$MatrixOfAccessRights:

$$\text{MatrixOfAccessRights} = \begin{vmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{vmatrix} \quad (4.8)$$

Дамо коротке пояснення даним наведеної матриці MatrixOfAccessRights.

З матриці прав доступу (4.8) можна побачити, що користувачу $\text{Subject}_1 \in \text{SUBJECTS}$ заздалегідь заблоковано доступ до ресурсів Object_2, Object_4, Object_5, Object_6, Object_7, Object_8, про що свідчить $AR_{1,2}=AR_{1,4}=AR_{1,5}=AR_{1,6}=AR_{1,7}=AR_{1,8}=0$ ($AR_{ij} \in$ MatrixOfAccessRights).

Також з матриці MatrixOfAccessRights та $BC_9 \in$ VectorOfBoundaryConstraints і $BC_{10} \in$ VectorOfBoundaryConstraints слідує необмежений доступ для всіх зареєстрованих користувачів $\text{Subject}_i \in \text{SUBJECTS}$ до ресурсів Object_9 і Object_{10}, оскільки $BC_9=0$, $BC_{10}=0$, $AR_{i9}=1$ і $AR_{i10}=1$ ($AR_{i9} \in$ MatrixOfAccessRights і $AR_{i10} \in$ MatrixOfAccessRights, $i=1\ldots10$).

Доступ до ресурсу Object_8 при мінімальній границі обмежень прав доступу $BC_8=0$ ($BC_8 \in$ VectorOfBoundaryConstraints) для користувачів $\text{Subject}_1 \in \text{SUBJECTS}$ і $\text{Subject}_4 \in \text{SUBJECTS}$ є забороненим, про що свідчать $AR_{1,8}=0$ і $AR_{4,8}=0$ ($AR_{1,8} \in$ MatrixOfAccessRights і $AR_{4,8} \in$ MatrixOfAccessRights).

Доступ до ресурсу Object_7 має найсуттєвіші обмеження прав доступу як за високим рівнем границі обмежень прав доступу $BC_7=0.98$, так і через блокування прав доступу до нього для користувачів $\text{Subject}_1 \in \text{SUBJECTS}$, $\text{Subject}_2 \in \text{SUBJECTS}$, $\text{Subject}_4 \in \text{SUBJECTS}$, $\text{Subject}_6 \in \text{SUBJECTS}$ і

$Subject_8 \in SUBJECTS$, про що свідчать $AR_{1,7}=0$, $AR_{2,7}=0$, $AR_{4,7}=0$ $AR_{6,7}=0$, $AR_{8,7}=0$ і $AR_{10,7}=0$ ($AR_{i,7} \in MatrixOfAccessRights$).

Початкове лімітування прав доступі з допомогою вектора граничних обмежень прав доступу VectorOfBoundaryConstraints і матриці прав доступу MatrixOfAccessRights визначається адміністраторами системи або посадовими особами з відповідними повноваженнями з урахуванням політики безпеки корпорації і не є предметом даної роботи.

На цьому етапі етап підготовки вхідних даних для реалізації методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри є завершеним і метод починає свою роботу. Система контролю доступу працює на основі матриці прав доступу MatrixOfAccessRights і надає інформацію щодо дій користувачів методу для накопичення і обробки статистичних даних (рисунок 4.2).

Рисунок 4.2 – Робота методу з корпоративною мережею

З рисунку 4.2 видно, що подальша робота методу полягає в обробці і аналізі статистичних даних.

Для накопичення статистичних даних методом використовуються дві матриці математичної моделі – матриця санкціонованих дій

MatrixOfAuthorizedActions (2.5) і матриця заборонених дій MatrixOfProhibitedActions (2.6).

На підставі описів (2.5) і (2.6) та обмежень (4.2) і (4.4) зазначені матриці будуть мати розмірність 10×10 і узагальнене представлення:

$$\text{MatrixOfAuthorizedActions} = \begin{vmatrix} AA_{1,1} & AA_{1,2} & \cdots & AA_{1,10} \\ AA_{2,1} & AA_{2,2} & \cdots & AA_{2,10} \\ \vdots & \vdots & & \vdots \\ AA_{10,1} & AA_{10,2} & \cdots & AA_{10,10} \end{vmatrix}, \quad (4.9)$$

$$\text{MatrixOfProhibitedActions} = \begin{vmatrix} PA_{1,1} & PA_{1,2} & \cdots & PA_{1,10} \\ PA_{2,1} & PA_{2,2} & \cdots & PA_{2,} \\ \vdots & \vdots & & \vdots \\ PA_{10,1} & PA_{10,2} & \cdots & PA_{10,10} \end{vmatrix}. \quad (4.10)$$

На початку роботи методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри всі елементи матриці санкціонованих дій $AA_{ij} \in$ MatrixOfAuthorizedActions і матриці заборонених дій $PA_{ij} \in$ MatrixOfProhibitedActions мають нульові значення накопичених статистичних даних, тому заглиблюватись в деталізацію наповнення наповнення цих матриць не будемо.

В ході експерименту і накопичення його статистичної інформації дані матриць санкціонованих і заборонених дій динамічно оновлюються, що ускладнює повну презентацію змін їх значень. Для демонстрації ходу експерименту зроблено зрізи зазначених матриць в моменти фіксації порушень вимог політики безпеки. Для експерименту обрано найпростішу модель порушень вимог політики безпеки, в якій як порушення фіксувалися лише виявлені і заблоковані системою спроби користувачів $\text{Subject}_i \in$ SUBJECTS здійснення доступу до ресурсів $\text{Object}_j \in$ OBJECTS корпоративної мережі, до яких прав доступу у $\text{Subject}_i \in$ SUBJECTS немає (AR_{ij}=0, $AR_{ij} \in$ MatrixOfAccessRights).

Перший зріз даних матриць відображує фіксацію першого порушення в системі:

$$\text{MatrixOfAuthorizedActions} = \begin{vmatrix} 5 & 0 & 18 & 0 & 0 & 0 & 0 & 0 & 23 & 3 \\ 0 & 12 & 1 & 0 & 0 & 1 & 0 & 5 & 6 & 7 \\ 21 & 0 & 32 & 0 & 0 & 0 & 6 & 41 & 0 & 12 \\ 0 & 0 & 0 & 84 & 0 & 10 & 0 & 0 & 0 & 0 \\ 11 & 7 & 0 & 1 & 0 & 0 & 1 & 5 & 0 & 0 \\ 0 & 19 & 0 & 57 & 0 & 7 & 0 & 25 & 3 & 0 \\ 0 & 0 & 0 & 19 & 52 & 0 & 0 & 0 & 1 & 0 \\ 0 & 12 & 10 & 21 & 14 & 0 & 12 & 1 & 7 & 1 \\ 11 & 0 & 19 & 41 & 0 & 17 & 0 & 14 & 1 & 1 \\ 54 & 8 & 21 & 15 & 0 & 0 & 0 & 0 & 12 & 1 \end{vmatrix}, \quad (4.11)$$

$$\text{MatrixOfProhibitedActions} = \begin{vmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{vmatrix}, \quad (4.12)$$

Порушення відображене в матриці заборонених дій MatrixOfProhibitedActions $PA_{3,4}$=1 і фіксує спробу несанкціонованого ($AR_{3,4}$=0, $AR_{3,4}$∈MatrixOfAccessRights) доступу користувача Subject_3∈SUBJECTS до ресурсу Object_4∈OBJECTS.

Порушення політики безпеки має наслідком зміну значення $P(\text{AuthorizedActions})_3$ імовірнісного критерія довіри до користувача Subject_3∈SUBJECTS у векторі VectorOfTrustCriteria (4.13) згідно (2.7).

$$\text{VectorOfTrustCriteria} = \begin{vmatrix} 1 \\ 1 \\ 0.991 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{vmatrix}. \quad (4.13)$$

Значення імовірнісного критерія довіри $P(\text{AuthorizedActions})_3$=0.991 не обмежує для користувача $\text{Subject}_3 \in$SUBJECTS можливостей доступу до ресурсів $\text{Object}_i \in$OBJECTS, оскільки значення $BC_j \in$VectorOfBoundaryConstraints мають менші граничні обмеження.

Наступний зріз даних матриць (4.14), (4.15) демонструє першу фіксацію умов блокування прав доступу користувача до ресурсу корпоративної мережі, що відображує вектор критеріїв довіри VectorOfTrustCriteria (4.16):

$$\text{MatrixOfAuthorizedActions} = \begin{vmatrix} 30 & 0 & 56 & 0 & 0 & 0 & 0 & 0 & 68 & 5 \\ 0 & 24 & 9 & 7 & 5 & 21 & 0 & 18 & 23 & 12 \\ 47 & 0 & 89 & 0 & 0 & 0 & 12 & 54 & 12 & 18 \\ 7 & 0 & 0 & 129 & 28 & 41 & 0 & 0 & 5 & 8 \\ 17 & 19 & 12 & 20 & 0 & 0 & 11 & 12 & 5 & 5 \\ 0 & 29 & 7 & 79 & 27 & 14 & 0 & 30 & 10 & 3 \\ 0 & 0 & 0 & 25 & 79 & 0 & 0 & 12 & 15 & 7 \\ 0 & 25 & 21 & 27 & 19 & 0 & 21 & 8 & 15 & 2 \\ 17 & 12 & 30 & 54 & 5 & 21 & 5 & 14 & 3 & 2 \\ 59 & 9 & 39 & 19 & 0 & 0 & 0 & 0 & 15 & 6 \end{vmatrix} \quad (4.14)$$

$$\text{MatrixOfProhibitedActions} = \begin{vmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{vmatrix}, \quad (4.15)$$

$$\text{VectorOfTrustCriteria} = \begin{vmatrix} 1 \\ 1 \\ 0.996 \\ 1 \\ 1 \\ 1 \\ 0.992 \\ 0.978 \\ 1 \\ 1 \end{vmatrix}. \quad (4.16)$$

Третій зріз даних матриць (4.17), (4.18) і вектор критеріїв довіри VectorOfTrustCriteria (4.19) демонструє дані роботи методу на фінал експерименту:

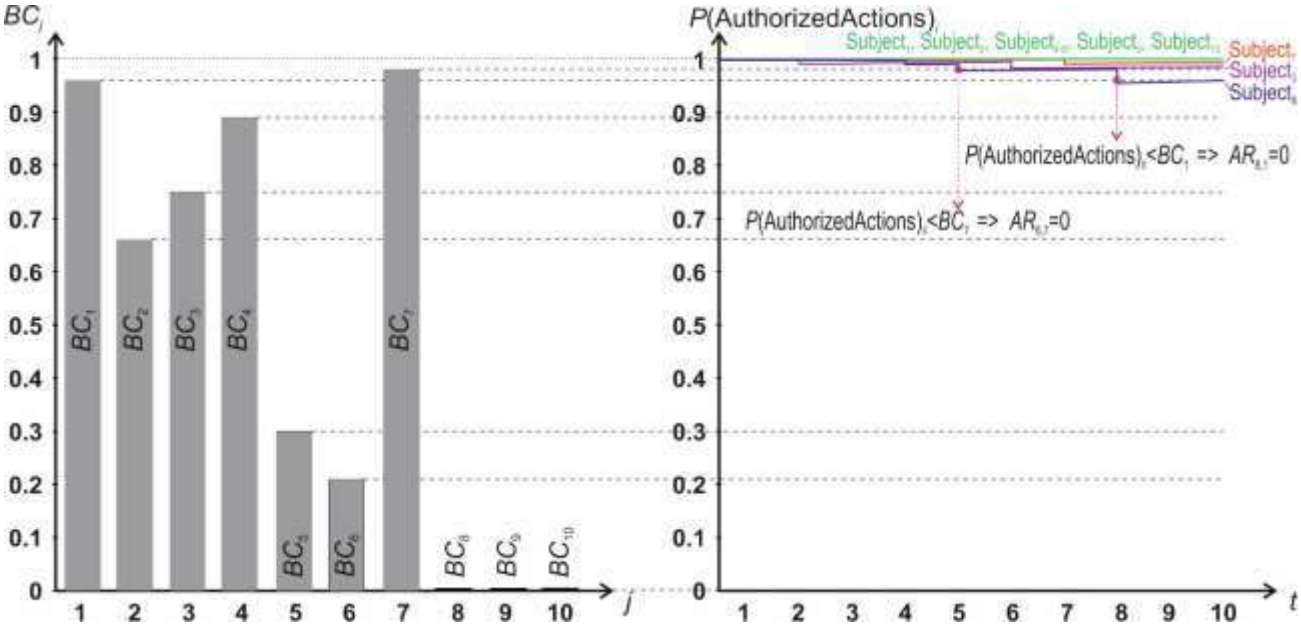
$$\text{MatrixOfAuthorizedActions} = \begin{vmatrix} 41 & 0 & 66 & 0 & 0 & 0 & 0 & 0 & 89 & 7 \\ 0 & 30 & 12 & 8 & 7 & 27 & 0 & 21 & 26 & 14 \\ 57 & 0 & 93 & 0 & 0 & 0 & 16 & 75 & 14 & 19 \\ 9 & 0 & 0 & 138 & 37 & 41 & 0 & 0 & 9 & 11 \\ 21 & 27 & 14 & 25 & 0 & 0 & 16 & 14 & 6 & 5 \\ 0 & 33 & 12 & 93 & 29 & 18 & 0 & 39 & 12 & 5 \\ 0 & 0 & 0 & 28 & 84 & 0 & 0 & 19 & 21 & 12 \\ -3 & 27 & 23 & 30 & 24 & 0 & 21 & 12 & 18 & 3 \\ 21 & 14 & 39 & 57 & 14 & 28 & 9 & 17 & 5 & 3 \\ 66 & 12 & 48 & 30 & 0 & 0 & 0 & 0 & 21 & 7 \end{vmatrix} \quad (4.17)$$

$$\text{MatrixOfProhibitedActions} = \begin{vmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 & 0 & 5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{vmatrix}, \quad (4.18)$$

$$\text{VectorOfTrustCriteria} = \begin{vmatrix} 1 \\ 1 \\ 0.982 \\ 1 \\ 1 \\ 1 \\ 0.994 \\ 0.958 \\ 1 \\ 1 \end{vmatrix}. \quad (4.19)$$

На рисунку 4.3 представлені презентаційні діаграми, які демонструють роботу методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри в ході реалізації експерименту.

Перша діаграма (рисунок 4.3.а) відображує представлення вектора граничних обмежень VectorOfBoundaryConstraints (4.5). Друга діаграма (рисунок 4.3.б) відображує динамічну зміну вектора критеріїв довіри VectorOfTrustCriteria.



а) б)

Рисунок 4.3 – Діаграми презентації результатів експерименту:
а – вектор граничних обмежень VectorOfBoundaryConstraints;
б – зміна вектора критеріїв довіри VectorOfTrustCriteria

На діаграмі 4.3.б акцентовано два моменти зниження критерія довіри користувача $Subject_8 \in SUBJECTS$ нижче за задані обмеження вектора граничних обмежень VectorOfBoundaryConstraints для ресурсів $Object_7 \in OBJECTS$ і $Object_1 \in OBJECTS$, наслідком чого є блокування доступу користувача $Subject_3 \in SUBJECTS$ до зазначених ресурсів через обнуління значень

$AR_{8,7} \in$ MatrixOfAccessRights і $AR_{8,1} \in$ MatrixOfAccessRights відповідно до визначених системою (2.3) правил. Аналіз початкової матриці заборонених дій MatrixOfProhibitedActions (4.8) експерименту показує, що $AR_{8,1} \in$ MatrixOfAccessRights в ній вже встановлене як $AR_{8,1}=0$, що не змінює права доступу $\text{Subject}_8 \in$ SUBJECTS до ресурсу $\text{Object}_1 \in$ OBJECTS, але отримання $P(\text{AuthorizedActions})_8 < BC_7$ призводить до зміни $AR_{8,7}=1$ на $AR_{8,7}=0$ і тим самим блокує доступ користувача $\text{Subject}_8 \in$ SUBJECTS до ресурсу $\text{Object}_7 \in$ OBJECTS.

На фінальному етапі експерименту матриця заборонених дій MatrixOfProhibitedActions має вигляд:

$$\text{MatrixOfAccessRights} = \begin{vmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{vmatrix}. \quad (4.20)$$

З діаграмі 4.3.б також видно, що коректні дії «користувачів-порушників» поступово відновлюють довіру до них і $P(\text{AuthorizedActions})_i \in$ VectorOfTrustCriteria поступово зростає з перспективою наближення до одиниці (граничної верхньої межі $P(\text{AuthorizedActions})_i$). За таких умов стає можливим відновлення $P(\text{AuthorizedActions})_8$ $P(\text{AuthorizedActions})_8 \geq BC_7$, але це не призводить до автоматичної протилежної зміни $AR_{8,7}=0$ на $AR_{8,7}=1$ і відновлення прав доступу користувача $\text{Subject}_8 \in$ SUBJECTS до ресурсу $\text{Object}_7 \in$ OBJECTS.

Відновлення прав доступу користувача $Subject_i \in SUBJECTS$ до будь-якого ресурсу $Object_j \in OBJECTS$ серйозного підходу і аналізу інцидентів, що зумовили зниження довіри користувача. За результатами аналізу статистику хибних дій користувача може бути обнулено або скореговано і доступ до ресурсів переглянуто, що є прерогативою відповідних служб корпорації і не є предметом даної роботи.

4.3 Висновки

В четвертому розділі презентовано можливості і здійснено апробацію методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри.

В розділі здійснене дослідження актуальних загроз безпеці інформаційних ресурсів корпоративної мережі і можливостей запропонованого методу щодо протидії виявленим загрозам.

Проведена експериментальна апробація методу, що має за мету демонстрацію принципів застосування методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри та підтвердження дієвості методу.

Результати проведеного експерименту повністю відповідають очікуваним і підтверджують на практиці дієвість теоретичних положень методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри.

В плані розширення функціональності методу матриця прав доступу MatrixOfAccessRights може бути переведена з булевого типу в матрицю з багаторівневою градацією прав доступу до кожного інформаційного ресурсу, що є предметом подальших досліджень з вдосконалення методу.

ВИСНОВКИ

В роботі за результатами теоретичних й практичних досліджень здійснено розробку методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри. При розробці методу переслідувалась мета, що полягає у вдосконаленні технологій захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу за рахунок оцінки імовірності виникнення загроз і попередження несанкціонованих дій користувачів на основі накопичуваних статистичних даних.

Згідно програми досліджень виконано наступні роботи:

– проведене дослідження корпоративних мереж як об’єкту інформаційної безпеки, в ході якого були досліджені принципи організації корпоративних мереж та типові загрози безпеці інформаційних ресурсів і виявлено перспективні напрямки та способи вдосконалення захисту інформаційних ресурсів корпоративної мережі на основі статистичних даних про дії користувачів;

– визначено основні положення методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри;

– розроблено математичну модель методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри, запропоновано оригінальну концепцію реалізації методу в термінах математичної моделі;

– розроблено узагальнений і деталізований алгоритми реалізації методу;

– здійснено апробацію дієвості прийнятих теоретичних і алгоритмічних рішень методу.

Оцінка отриманих результатів дозволила дійти загального висновку, що в роботі виконані всі поставлені задання і досягнуто загальної мети дослідження.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Чинчик Д., Коробейнікова Т., Захарченко С. Методи та засоби комплексного захисту корпоративної мережі. InterConf. 2021. №84. С. 433-450.

2. Азарова А. О., Білий Р. О. Аналіз базових концепцій розподіленої корпоративної мережі. Конференція ВНТУ, 2021. С.128-129.

3. Трояновська Т.І., Вініченко Д.О. Корпоративна мережа, як засіб організації роботи підприємства. Конференція ВНТУ, 2017. С.102-105.

4. Мультивендорна корпоративна мережа: міфи і реальність Блог про все цікаве у світі телекомунікацій. URL: https://www.telesphera.net/blog/corporate-network.html (дата звернення: 09.09.2023).

5. Корунський Є. С. Методика оцінки ресурсів мультисервісної корпоративної мережі, необхідних для забезпечення заданої якості обслуговування. URL: https://ppt-online.org/181173 (дата звернення: 21.09.2023).

6. Слінько Т. Сучасні загрози інформаційній безпеці країни та шляхи їх подолання Український часопис конституційного права. 2021. №4. С. 77-84.

7. Стандарти інформаційної безпеки. URL: https://coggle.it/diagram/X7jnwVJoLGbJ6MVK/t/стандарти-інформаційної-безпеки (дата звернення: 30.09.2023).

8. Дикий О. В., Флюнт М. О. Стандарти інформаційної безпеки: компаративне дослідження. Право та державне управління. 2019. № 2 (35), том 1. С. 80-87.

9. Крюгер Г. Стандарти інформаційної безпеки - огляд. dqsglobal. 2022. URL: https://www.dqsglobal.com/uk-ua/navchajtesya/blog/standarti-informacijnoyi-bezpeki-oglyad (дата звернення: 30.09.2023).

10. Курило А.Г. Міжнародно-правові стандарти забезпечення права особи на інформаційну безпеку. Вісник національного університету цивільного захисту України, Серія "Державне управління". 2021. № 2(15). С. 117-123.

11. Livshitz I.I., Neklyudov A.V., Lontsikh P.A. Evaluation of IT security – genesis and its state-of-art. International Conference Information Technologies in

Business and Industry 2018. IOP Publishing. 2018. C. 1-7.

12. Lawrence C. Miller and Peter H. Gregory. Evaluation Criteria of Systems Security Controls. CISSP Articles. 2018. URL: https://www.dummies.com/article/academics-the-arts/study-skills-test-prep/cissp/evaluation-criteria-systems-security-controls-254878/ (дата звернення: 30.09.2023).

13. Abhi G. CISSP Concepts – Trusted Computing Base/ TCEC, ITSEC and Common Criteria. Cyber Management Alliance Articles. Jan 28, 2020. URL: https://www.cm-alliance.com/cissp/trusted-computing-base/-tcec-itsec-and-common-criteria (дата звернення: 30.09.2023).

14. Randal Allen. Evolved Artificial Intelligence for Stochastic Clustering Unsupervised Learning. Interservice/Industry Training, Simulation, and Education Conference. 2020. Paper № 20258. 8 p.

15. Гапак О. М., Балога С.І. Захист інформації в комп'ютерних системах: підручник. Ужгород: ДВНЗ «Ужгородський НУ», 2021. 184 с.

16. Міжнародна економічна безпека України: теорія, методологія, практика: монографія. / за наук. ред. доц. Кравчука П.Я. Луцьк : ІВВ Луцького НТУ, 2020. 212с.

17. The Canadian Trusted Computer Product Evaluation Criteria 3rd Ed. CTCPEC Version 3.0e. Publisher: Communications Security Establishment, 1993. Last modified: April 15, 2022. 208 p.

18. Donald P. Kommersю The Basic Law: A Fifty Year Assessment. German Law Journal. 2019. Volume 20, Issue 4. P. 571-582.

19. Ayhan, E., Lahdili N. Federal Republic of Germany. The Palgrave Handbook of Comparative Public Administration. Singapore: Palgrave Macmillan, 2022. URL: https://doi.org/10.1007/978-981-19-1208-5_8 (дата звернення: 30.09.2023).

20. Турчак А. Основні складові інформаційної безпеки держави Аспекти публічного управління. Том 7, № 5. 2019. С. 44-56.

21. Defining Security Requirements with the Common Criteria: Applications, Adoptions, and Challenges / Nan Sun et al. Computer Science - Cryptography and

Security. 2022. V.1. P. 44756-44777.

22. A survey on common criteria (CC) evaluating schemes for security assessment of IT products / Chang-Tsun Li et al. PeerJ Comput Sci. 2021. №7. 22p.

23. Maheen Fatima, Haider Abbas. Germany's Federal Debt Rule (Debt Brake). Germany: Federal Ministry of Finance, 2022. 38p.

24. Карпович І.М., Гладка О.М., Наконечна Ю.А. Аналіз ризиків безпеки інформаційної системи ІТ-підприємства. Вчені записки ТНУ імені В.І. Вернадського. Серія: технічні науки. 2020. Том 31 (70) № 5. С. 69-74.

25. Бурячок В. Л. , Киричок Р. В., Складанний П. М. Основи інформаційної та кібернетичної безпеки: навчальний посібник. К. , 2018. 320 с.

26. Петренко К.М. Удосконалена методика оцінювання ефективності системи забезпечення інформаційної безпеки Міністерства оборони та збройних сил України. Сучасні інформаційні технології у сфері безпеки та оборони. 2022. № 3 (45). С. 97-100.

27. Petrenko K.M. An improved system of criteria and indicators for evaluating the effectiveness of the information security system of the Ministry of Defense and the Armed Forces of Ukraine. Works of the university. 2022. № 5(174). С. 180-186.

28. Батечко С.В., Лебедєва О.Ю., Зоріло В.В. Методика оцінки захищеності інформаційних систем. Інформатика та математичні методи в моделюванні. 2021. Том 11, № 3. С. 173-180.

29. Prat Namtien. Understanding the Importance of Network Security Assessments. LinkedIn. Published Jun 30, 2023. URL: https://www.linkedin.com/pulse/understanding-importance-network-security-assessments-prat-namtien (дата звернення: 12.10.2023).

30. Network Security Assessment: Protecting assets, preparing for attacks. Ciber 4 All Team. Jan – 2023. URL: https://www.tarlogic.com/blog/network-security-assessment/ (дата звернення: 12.10.2023).

31. Hongyu Yang, Renyun Zeng, Guangquan Xu, Liang Zhang. A network security situation assessment method based on adversarial deep learning. Applied Soft Computing. 2021. URL: https://www.sciencedirect.com/science/article/abs/pii/S1568494621000193

(дата звернення: 12.10.2023).

32. Network Security Assessments: How They Help Manage the Risk of a Cyberattack. Rapid Fire Tools. 2023. URL: https://www.rapidfiretools.com/blog/network-security-assessment/ (дата звернення: 30.09.2023).

33. Poorna Mohan. Network Security Assessment: What It is and its Benefits? Externetworks. 2022. URL: https://www.extnoc.com/blog/network-security-assessment-and-benefits/ (дата звернення: 30.09.2023).

34. Didmanidze Ibraim, Donadze Mikheil. Information Security System Evaluation Criteria in Educational Computer Networks. Cross-Cultural Studies: Education and Science. 2022. Vol. 7, Issue 3. P. 133-141.

35. Implementing "method of successive concessions" in selecting the optimal variant to protect a corporate network / Diallo A. et al. The Eurasian Scientific Journal. 2018. 11p.

36. David Hammarberg. SOC 2 Trust Service Criteria for Privacy. McKonly & Asbury. 2021. URL: https://macpas.com/soc-2-trust-service-criteria-for-privacy/ (дата звернення: 30.09.2023).

37. Kim Koch. How to Comply with Trust Services Criteria for SOC 2 Examinations. Moss Adams. 2022. URL: https://www.mossadams.com/articles/2021/07/soc-2-trust-services-criteria (дата звернення: 12.10.2023).

38. Про інформацію : Закон України від 2.10.1992р. № № 2657-XII : Редакція від 27.07.2023р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#doc_info (дата звернення: 11.10.2023).

39. Що таке юридична особа. URL: https://smarttender.biz/terminy/view/yurydychna-osoba/ (дата звернення: 11.10.2023).

40. Дорофеєва В.І. Конституційні засади участі громадських об’єднань в системі захисту прав людини: Україна та зарубіжний досвід : автореф. дисертації на здобуття наук. ступ. канд. юрид. наук: 12.00.02. Ужгород, 2018. 19 с.

41. Мельник Р.С. Адміністративне право і процес : теорія та практика правозастосування: монографія. Херсон: Видавничий дім «Гельветика», 2019. 212с.

42. Марченко П. А. Методи розмежування доступу в розподілених системах кешування даних. Магістерська дисертація. Київ: НТУ УКРАЇНИ «КПІ ім. І. Сікорського», 2018. 91 с.

43. Шемчук В.В. Загрози інформаційній безпеці: проблеми визначення та подолання. Експерт: парадигми юридичних наук і державного управління. 2020. №(7). С. 285-296.

44. Інформаційна безпека: види загроз і методи їх усунення. 2020 URL: https://datami.ua/informatsijna-bezpeka-vidi-zagroz-i-metodi-yih-usunennya/ (дата звернення: 21.09.2023).

45. Рой Я., Мазур Н., Рябчун О. Стратегія визначення гіпотетичного напряму підвищення рівня небезпеки загроз інформаційній безпеці. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2019. 3(3). С. 97-103.

46. Харченко С. О. Наукові підходи до класифікації загроз інформаційній безпеці. Серія: Державне управління. 2019. № 2 (66). С. 191-197.

47. Федорова Н.Є., Смєсова В.Л. Інформаційна безпека та шляхи її забезпечення на етапі інформаційно-технологічної революції. Причорноморські економічні студії. 2020. Випуск 57. С.13-16.

48. Дикий А. П., Наумчук К. М., Тростенюк Т. М. Аналіз сучасних загроз інформаційній безпеці держави. Економічний простір. 2021. №176. С.155-158.

49. Храпкін О.М. Захист інформаційно-комунікаційної мережі установи від несанкціонованого доступу. Системи озброєння і військова техніка. 2020. № 3(63). С.45-53.

50. Судова практика розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку. ВЕРХОВНИЙ СУД УКРАЇНИ - офіційний веб-сайт. URL: https://www.viaduk.net/clients/vsu/vsu.nsf/(documents)/AFB1E90622E4446FC2257 (дата звернення: 21.09.2023).

51. Pienta D., Tams S., Bennet Thatcher J. Can Trust be Trusted in Cybersecurity? Proceedings of the 53rd Hawaii International Conference on System Sciences, 2020. P. 4264-4273.

52. Малицький Т.Б., Чешун О.В., Чешун В.М. Математична інтерпретація концепції захисту інформаційних ресурсів корпоративної мережі із застосуванням імовірнісних критеріїв довіри. Збірник наукових праць за матеріалами XV Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2023». Хмельницький. 2023. С.172-176.

53. Малицький Т.Б., Чешун О.В., Чешун В.М. Критерії довіри безпеки корпоративних мереж. Військова освіта і наука: сьогодення та майбутнє : зб. тез доповідей XIX Міжнародної науково-практичної конференції, м. Київ, 10.11.2023 р. Київ : Військовий інститут Київського національного університету імені Тараса Шевченка, 2023. С. 47.

54. Малицький Т.Б., Чешун О.В., Чешун В.М. Алгоритм роботи системи захисту інформаційних ресурсів мережі із застосуванням критеріїв довіри. Електронні інформаційні ресурси: створення, використання, доступ. Збірник матеріалів Міжнародної науково-практичної Інтернет конференції, 20-21.11.2023 р. Суми/Вінниця: НІКО/ КЗВО «Вінницька академія безперервної освіти», 2023. С.54-56.

АКТУАЛЬНІ ПРОБЛЕМИ КОМП'ЮТЕРНИХ НАУК - 2023

XV Всеукраїнська науково-практична конференція

Метою конференції є висвітлення актуальних проблем комп'ютерних наук, інформатики та інформаційних технологій.

СЕКЦІЇ КОНФЕРЕНЦІЇ:

1. Комп'ютерні науки та прикладні інформаційні технології.
2. Комп'ютерна інженерія та системи захисту інформації.
3. Математичне моделювання та інженерія програмного забезпечення
4. Телерадіокомунікації, медійні та комунікаційні системи.
5. Проблеми впровадження інформаційних технологій у виробництво та управління.

Робочі мови конференції: українська, англійська

ОРГКОМІТЕТ:

Олег СИНЮК – голова оргкомітету, проректор Хмельницького національного університету з наукової роботи, доктор технічних наук, професор

Олег САВЕНКО – заступник голови оргкомітету, декан факультету Інформаційних технологій ХНУ, доктор технічних наук, професор

Олександр БАРМАК – заступник голови оргкомітету, завідувач кафедри Комп'ютерних наук ХНУ, доктор технічних наук, професор

Тетяна ГОВОРУЩЕНКО – завідувач кафедри Комп'ютерної інженерії та інформаційних систем ХНУ, доктор технічних наук, професор

Олена ВИСОЦЬКА – доктор технічних наук, завідувач кафедри Радіоелектронних та біомедичних комп'ютеризованих засобів і технологій Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут», професор

Євгеній ЛАВРОВ – доктор технічних наук, професор (Сумський державний університет)

Людмила ТІМОФЄЄВА – відповідальна за студентську науково-дослідну роботу ХНУ

Олександр МАЗУРЕЦЬ – секретар конференції, к.т.н., доцент кафедри Комп'ютерних наук ХНУ

Марина МОЛЧАНОВА – секретар конференції, викладач кафедри Комп'ютерних наук ХНУ

КОНТАКТНА ІНФОРМАЦІЯ:

e-mail для листування: *apkt.khnu@gmail.com*

УДК 004.056.5

Малицький Т.Б., Чешун О.В., Чешун В.М.

Хмельницький національний університет

МАТЕМАТИЧНА ІНТЕРПРЕТАЦІЯ КОНЦЕПЦІЇ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ КОРПОРАТИВНОЇ МЕРЕЖІ ІЗ ЗАСТОСУВАННЯМ ІМОВІРНІСНИХ КРИТЕРІЇВ ДОВІРИ

Розглянуто концептуальні положення методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу із застосуванням імовірнісних критеріїв довіри, наведено базові положення методу та загальний опис математичної моделі, представлено концепцію реалізації методу в термінах запропонованої математичної моделі.

The conceptual provisions of the method of protecting information resources of the corporate network from unauthorized access based on probabilistic assessments of trust criteria are considered, the basic provisions of the method and a general description of the mathematical model are given, and the concept of method implementing in terms of the proposed mathematical model is presented.

В умовах все більшого поширення та інтелектуалізації цифрових технологій та зростання кіберзагроз безпека корпоративних мереж стає важливою складовою сучасного бізнесу. Досягнення ефективної безпеки корпоративних мереж вимагає комплексного підходу, враховуючи технологічні інновації та ретельний аналіз потенційних загроз [1]. Технологічні інновації охоплюють сукупність організаційних та програмно-апаратних безпекових заходів [2,3]: міжмережеві екрани, антивірусне програмне забезпечення, шифрування даних; аутентифікація та авторизація; навчання персоналу; регулярні оновлення та патчі; резервне копіювання та відновлення даних, моніторинг та аналіз активності мережі.

Одним із ключових заходів інформаційної безпеки корпоративних мереж є моніторинг та аналіз активності мережі та блокування шкідливих дій з її ресурсами [4]. Постійний моніторинг мережі і виявлення загроз допомагають вчасно реагувати на кібератаки та аномальну активність, запобігаючи можливим інцидентам. Проблема бокування шкідливих дій полягає не безпосередньо в операції блокування, а у прогнозуванні зловмисності дій, тобто, в оцінці «довіри» до ініціатора цих дій. Довіра в інформаційній безпеці є ключовим аспектом для забезпечення захисту конфіденційної інформації та інфраструктури [5]. Щоб оцінити рівень довіри в інформаційній безпеці потрібні критерії визначення, наскільки ефективно застосовуються заходи безпеки та враховуються ризики.

Проведені дослідження свідчать на користь використання в якості критерію

довіри суб'єктів взаємодії в інформаційному просторі корпоративної мережі імвірнісного показника, що формується на основі накопичуваної статистики попередньої діяльності кожного субєкта із урахуванням зафіксованих випадків шкідливої активності відносно загального показника активності.

Концепція методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу із застосуванням імовірнісних оцінок критеріїв довіри базується на положеннях:

– метод розробляється для підвищення ефективності захисту інформаційних ресурсів мережі від несанкціонованого доступу;

– метод базується на виявленні аномальної поведінки користувачів інформаційних ресурсів корпоративної мережі і обмеженні прав доступу до зазначених ресурсів при виявленні порушень користувачем вимог політики безпеки роботи в мережі;

– реагування на порушеня користувачем вимог політики безпеки роботи в корпоративній мережі з прийняттям рішення щодо обмеження доступу до її інформаційних ресурсів здійснюється системою захисту інформації автоматично в реальному масштабі часу;

– реалізація методу захисту інформаційних ресурсів корпоративної мережі в реальному масштабі часу системою захисту без втручання людини зумовлює потребу у використанні чітко визначеного математичного базису та правил роботи методу на основі цього базису, що є основою для алгоритмічної і подальшої технічної (програмної) реалізації методу;

– математичною основою методу є визначена ймовірнісна статистична математична модель управління доступом на основі концепції (критеріїв) довіри;

– базовим критерієм для динамічного управління розподілом прав доступу є імовірнісний критерій довіри, що розраховується і постійно динамічно корегується з урахуванням активності користувача в мережі;

– імовірнісний критерій довіри до користувача є основним при визначенні і зміні прав користувача на доступ до інформаційних ресурсів корпоративної мережі та при автоматичному блокуванні доступу користувача до зазначених ресурсів тощо.

Розроблена в термінах математичної моделі структурно-логічна схема реалізації концепції методу представлена на рисунку 1.

Методики, прийоми та засоби, які використовуються для збору статистичних даних щодо поведінки користувачів, їх аналізу і обробки, алгоритми виконання конкретних завдань у рамках методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу із застосуванням імовірнісних оцінок критеріїв довіри засновані на ймовірнісній статистичній математичній моделі управління доступом на основі концепції (критеріїв) довіри.

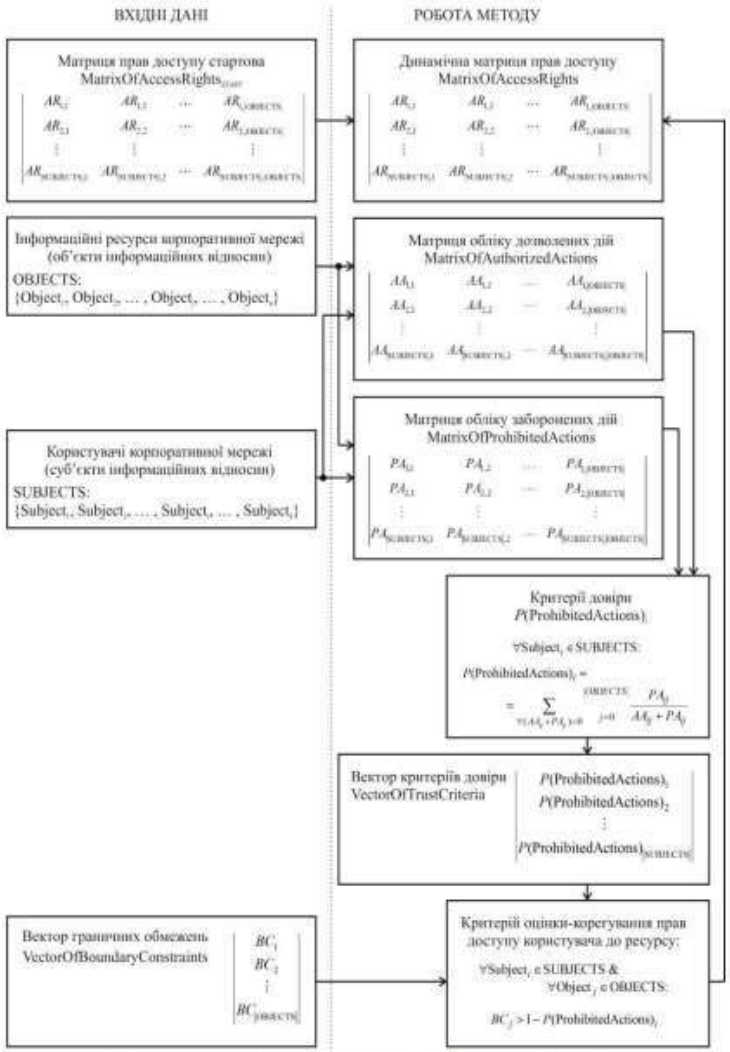


Рисунок 1 – Структурно-логічна схема реалізації концепції методу в термінах математичної моделі

Метод базується на аналізі характеру дій (активностей) користувачів інформаційних ресурсів, що в математичній моделі розглядається як взаємодія зазначених суб'єктів і об'єктів інформаційних відносин, відображених в моделі множинами SUBJECTS і OBJECTS відповідно.

Базовим елементом визначення прав доступу користувачів $Subject_i \in SUBJECTS$ до інформаційних ресурсів $Object_j \in OBJECTS$ корпоративної мережі є бінарна матриця прав доступу MatrixOfAccessRights.

Базовим критерієм для динамічного управління розподілом прав доступу є імовірнісний критерій довіри $P(\text{ProhibitedActions})_i$, що розраховується і постійно динамічно корегується з урахуванням активності користувача $Subject_i \in SUBJECTS$ в мережі, яка зводиться до статистики дій користувача корпоративної мережі.

Накопичувані статистичні дані щодо дій суб'єктів $Subject_i \in SUBJECTS$ інформаційних відносин над об'єктами $Object_j \in OBJECTS$ корпоративної мережі формуються з розподілом даних щодо дій користувачів на коректні і некоректні з точки зору дотримання вимог політики безпеки роботи в мережі та узагальнюються в моделі у формі матриць санкціонованих дій MatrixOfAuthorizedActions і заборонених дій MatrixOfProhibitedActions.

Імовірнісний критерій довіри розраховується на основі накопичуваних статистичних даних щодо дій суб'єктів інформаційних відносин над об'єктами (інформаційними ресурсами) корпоративної мережі (даних матриці санкціонованих дій MatrixOfAuthorizedActions і матриці заборонених дій MatrixOfProhibitedActions) і узагальнюється для всіх користувачів $Subject_i \in SUBJECTS$ інформаційних ресурсів корпоративної мережі в формі вектора критеріїв довіри VectorOfTrustCriteria.

Вектор критеріїв довіри VectorOfTrustCriteria до користувачів $Subject_i \in SUBJECTS$ інформаційних ресурсів корпоративної мережі, який, фактично, є відображенням статистичної імовірності несакціонованих дій користувача $Subject_i \in SUBJECTS$ в полі OBJECTS інформаційних ресурсів корпоративної мережі, передбачається до використання як основний критерій довіри методу захисту інформаційних ресурсів корпоративної мережі і як інструмент динамічного управління правами доступу користувачів до ресурсів корпоративної мережі.

Для реалізації динамічного управління правами доступу користувачів $Subject_i \in SUBJECTS$ до ресурсів $Object_j \in OBJECTS$ корпоративної мережі використовуються рівні обмеження довірчого допуску до кожного інформаційного ресурсу $Object_j \in OBJECTS$, систематизовані у вигляді вектора граничних обмежень VectorOfBoundaryConstraints довірчого допуску до ресурсів мережі.

Якщо відображувана вектором критеріїв довіри VectorOfTrustCriteria статистика дій певного користувача $Subject_i \in SUBJECTS$ в полі OBJECTS інформаційних ресурсів корпоративної мережі призводить до падіння рівня його довіри нижче за обмеження довірчого допуску до певного інформаційного ресурсу $Object_j \in OBJECTS$ корпоративної мережі, то доступ відповідного користувача до цього ресурсу блокується.

Блокування доступу користувача $Subject_i \in SUBJECTS$ до інформаційного ресурсу $Object_j \in OBJECTS$ передбачає зміну статусу зазначеного в матриці прав доступу MatrixOfAccessRights рівня прав доступу користувача – зміну значення елемента $AR_{ij} \in MatrixOfAccessRights$ на нульове. Умова $AR_{ij}=0$, відповідно, блокує доступ користувача $Subject_i \in SUBJECTS$ до інформаційного ресурсу $Object_j \in OBJECTS$.

Перелік посилань

1. Карпович І.М., Гладка О.М., Наконечна Ю.А. Аналіз ризиків безпеки інформаційної системи ІТ-підприємства. Вчені *записки ТНУ імені В.І. Вернадського. Серія: технічні науки*. 2020. Том 31 (70) № 5. С. 69-74.
2. Чинчик Д., Коробейнікова Т., Захарченко С. Методи та засоби комплексного захисту корпоративної мережі. *InterConf*, 2021, №84. С. 433-450.
3. Гапак О.М., Балога С.І. Захист інформації в комп'ютерних системах: підручник. Ужгород: Державний вищий навчальний заклад «Ужгородський НУ», 2021. 184 с.
4. Храпкін О.М. Захист інформаційно-комунікаційної мережі установи від несанкціонованого доступу. *Системи озброєння і військова техніка*. 2020. № 3(63). С.45-53.
5. Pienta D., Tams S., Bennet Thatcher J. Can Trust be Trusted in Cybersecurity? *Proceedings of the 53rd Hawaii International Conference on System Sciences*, 2020. P. 4264-4273.

Військова освіта і наука: сьогодення та майбутнє : зб. тез доповідей XIX Міжнародної науково-практичної конференції, м. Київ, 10 листопада 2023 р. Київ : Військовий інститут Київського національного університету імені Тараса Шевченка, 2023. 406 с.

Рекомендовано до друку Вченою радою Військового інституту Київського національного університету імені Тараса Шевченка
(протокол від 16.11.2023 № 3).

У збірнику тез доповідей друкуються матеріали виступів наукових і науково-педагогічних працівників, курсантів (студентів) Військового інституту Київського національного університету імені Тараса Шевченка та інших вищих військових та закладів вищої освіти України.

У публікаціях розглядаються: технічні проблеми озброєння і військової техніки та технології подвійного призначення; актуальні проблеми лінгвістичного забезпечення Збройних Сил України; актуальні питання військової психології та соціальної роботи; інформаційно-психологічна боротьба у воєнній сфері; інформаційно-медійне забезпечення МОУ та ЗСУ в умовах правового режиму воєнного стану; фінанси; актуальні проблеми військового права в умовах воєнного стану; актуальні проблеми геопросторової підтримки військ в умовах ведення російсько-української війни; наукові проблеми військової політології та морально-психологічного впливу

Малицький Т.Б. (ХмНУ)
Чешун О.В. (ХмНУ)
к.т.н., доц. Чешун В.М. (ХмНУ)

КРИТЕРІЇ ДОВІРИ БЕЗПЕКИ КОРПОРАТИВНИХ МЕРЕЖ

Безпека корпоративних мереж є важливою складовою сучасного бізнесу, особливо в умовах все більшого використання цифрових технологій та зростання кіберзагроз. Досягнення ефективної безпеки корпоративних мереж вимагає комплексного підходу, враховуючи технологічні інновації та ретельний аналіз потенційних загроз. Технологічні інновації охоплюють сукупність організаційних та програмно-апаратних безпекових заходів: міжмережеві екрани, антивірусне програмне забезпечення, шифрування даних; аутентифікація та авторизація; навчання персоналу; регулярні оновлення та патчі; резервне копіювання та відновлення даних, моніторинг та аналіз активності мережі.

Загалом, безпека корпоративних мереж є постійним процесом, який вимагає уваги до деталей та вдосконалення стратегій на основі новітніх ризиків та викликів кібербезпеки. Одним із ключових заходів інформаційної безпеки корпоративних мереж є моніторинг та аналіз активності мережі та блокування шкідливих дій з її ресурсами. Постійний моніторинг мережі і виявлення загроз допомагають вчасно реагувати на кібератаки та аномальну активність, запобігаючи можливим інцидентам. Проблема бокування шкідливих дій полягає не безпосередньо в операції блокування, а у прогнозуванні зловмисності дій, тобто, в оцінці «довіри» до ініціатора цих дій. Довіра в інформаційній безпеці є ключовим аспектом для забезпечення захисту конфіденційної інформації та інфраструктури. Щоб оцінити рівень довіри в інформаційній безпеці потрібні критерії, які допомагають визначити, наскільки ефективно застосовуються заходи безпеки та враховуються ризики.

Проведені дослідження свідчать на користь використання в якості критерію довіри суб'єктів взаємодії в інформаційному просторі корпоративної мережі імвірнісного показника, що формується на основі накопичуваної статистики попередньої діяльності кожного субєкта із урахуванням зафіксованих випадків шкідливої активності відносно загального показника активності. При цьому можуть бути використані різні коефіцієнти вагомості виявлних зловмисних або підозрілих дій і різні значення стартового порогу довіри для нового користувача. Чим нижчий рівень порогу довіри нового користувача і чим більші коефіцієнти ваги зловмисних/підозрілих дій, тим жорсткішою буде система захисту ресурсів мережі.

д.т.н., проф. Михайленко В.С (ОНУ)
д.т.н., проф. Гунченко Ю.О. (ОНУ)
Мартинович Л.Я. (ОНУ)

ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ ДАНИХ З ДОПОМОГЮ СПЕЦІАЛІЗОВАНОЇ ПРОГРАМИ ORANGE

Orange – це інструмент для візуалізації та аналізу даних з відкритим вихідним кодом. Orange розробляється в лабораторії біоінформатики на факультеті комп'ютерних та інформаційних наук Університету Любляни, Словенія разом із спільнотою відкритого вихідного коду. Також, Orange – це

УДК 004
ББК 32.97
Е50

Рекомендовано до видання Вченою радою КЗВО «Вінницька академія безперервної освіти» (протокол № 8 від 20.11.2023 р.)

Електронні інформаційні ресурси: створення, використання, доступ. Збірник матеріалів Міжнародної науково-практичної Інтернет конференції 20-21 листопада 2023 р. – Суми/Вінниця: НІКО/ КЗВО «Вінницька академія безперервної освіти», 2023. – 336 с.

ISBN 978-617-7422-23-4

Збірник містить матеріали Міжнародної науково-практичної Інтернет конференції «Електронні інформаційні ресурси: створення, використання, доступ. Матеріали збірника подано у авторській редакції. Автори опублікованих матеріалів несуть повну відповідальність за підбір, точність наведених фактів, цитат, статистичних даних, власних імен та інших відомостей, Матеріали відтворюються зі збереженням змісту, орфографії та синтаксису текстів, наданих авторами.

УДК 004
ISBN 978-617-7422-23-4

практиці, комбінація різних методів оптимізації може бути ефективною стратегією для розв'язання складних задач розподілу завдань в РІОС.

Список використаних джерел:

1. Голдберг В. Методи імітації відпалу в оптимізації / Вадим Голдберг. – Іздат, 2017. – 279 с.
2. Фаріма Ф. CAD для безпеки ПЗ: Огляд поточних проблем у сфері апаратної безпеки та ефективне використання CAD інструментів / Фаріма Ф. Сазадур Р – IEEE, 2023. – Видавництво, 2023. – 407 с.
3. Цінго Лю. Розподілена оптимізація в мережевих системах: Алгоритми та застосування / Цінго Лю, Сяофен Ляо, Хуацін Лі, Шаоцзян Ден, Шаньфу Гао – Springer Nature, 2023 – 289 с.
4. Чен Х., Шень М. Глибоке навчання з підкріпленням для планування FPGA HLS / Хонгженг Чен, Мінхуа Шень. – IEEE Transactions on CAD, 2020.
5. Огляд САПР до інтеграції CAE [Електронний ресурс] – Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/pii/S1018363920302282#:~:text=The%20developed%20CAD%20to%20CAE,to%20optimize%20the%20product%20model
6. Інноваційний підхід до еко-дизайну на основі інтеграції LCA, CAD\CAE [Електронний ресурс] – Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/abs/pii/S0959652618308904#:~:text=In%20this%20study%2C%20an%20innovative,CAD%2FCAE%20integration%20is%20briefly%20reviewed

МАЛИЦЬКИЙ Т.Б., ЧЕШУН О.В., ЧЕШУН В.М.,
Хмельницький національний університет

АЛГОРИТМ РОБОТИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ МЕРЕЖІ ІЗ ЗАСТОСУВАННЯМ КРИТЕРІЇВ ДОВІРИ

Анотація: В роботі представлено узагальнений алгоритм роботи системи захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу із застосуванням імовірнісних критеріїв довіри, наведено базові положення методики оцінювання та застосування рівня довіри до користувача у відповідності до запропонованого алгоритму та деталізовано принципи реалізації технології захисту ресурсів корпоративної мережі в термінах математичної моделі методу.

Ключові слова: захист інформації, корпоративна мережа, критерій довіри

Для реалізації ефективного захисту корпоративних мереж необхідно використовувати комплексний підхід, який враховує якісний аналіз потенційних загроз та сучасні інновації технологій протидії виявленим загрозам [1]. Серед традиційних способів протидії загрозам можна зазначити використання міжмережевих екранів, антивірусного програмного забезпечення, шифрування даних, навчання персоналу, проведення процедур автентифікації та авторизації, регулярні оновлення та використання патчів, здійснення резервного копіювання та відновлення даних, систематичний моніторинг та аналіз активності мережі тощо [2,3].

Одним з ключових заходів забезпечення інформаційної безпеки корпоративних мереж є проведення моніторингу та аналізу активності мережі з метою блокування шкідливих дій відносно її ресурсів [4]. Систематичний контроль мережі та виявлення можливих загроз дозволяють оперативно реагувати на кібератаки та аномальну активність, запобігаючи можливим інцидентам.

Проблема блокування шкідливих дій полягає не лише в самому акті блокування, але й в прогнозуванні зловмисності дій, тобто, в оцінці "довіри" до особи, що ініціює ці дії. У контексті інформаційної безпеки, довіра стає ключовим аспектом для гарантування захисту конфіденційної інформації та інфраструктури [5].

Пропонований підхід до організації захисту інформаційних ресурсів мережі із застосуванням критеріїв довіри базується на виявленні аномальної поведінки користувачів

інформаційних ресурсів корпоративної мережі і обмеженні прав доступу до зазначених ресурсів при виявленні порушень користувачем вимог політики безпеки роботи в мережі.

Основним критерієм для динамічного управління розподілом прав доступу є імовірнісний критерій довіри, що розраховується і постійно динамічно корегується з урахуванням активності користувача в мережі. Імовірнісний критерій довіри до користувача є основним при визначенні і зміні прав користувача на доступ до інформаційних ресурсів корпоративної мережі та при автоматичному блокуванні доступу користувача до зазначених ресурсів тощо.

Аналіз причинно-наслідкової схеми реалізації концепції довіри дозволяє виділити три основних фази роботи методу:

- підготовка вхідних даних та формування початкових представлень векторно-матричних складових реалізації методу;
- робота методу (реалізація інноваційної складової методу);
- взаємодія з мережею (використання результатів роботи методу для керування доступом до інформаційних ресурсів мережі та збір статистичних даних для наступних ітерацій реалізації інноваційної складової запропонованого підходу).

На рисунку 1 наведено блок-схему алгоритму роботи системи захисту інформаційних ресурсів мережі із застосуванням критеріїв довіри.

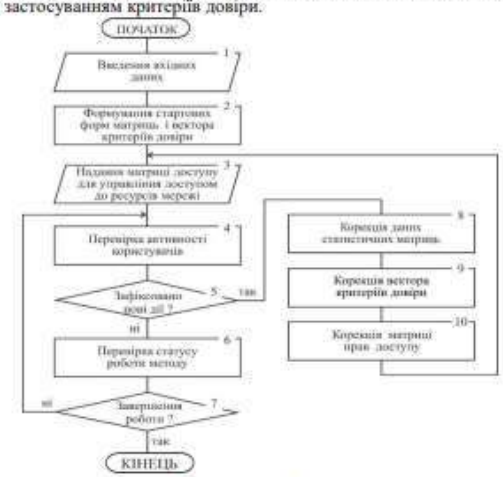


Рисунок 2 – Блок-схема узагальненого алгоритму роботи системи захисту

Базовим елементом визначення прав доступу користувачів до інформаційних ресурсів мережі є бінарна матриця прав доступу MatrixOfAccessRights. Критерієм динамічного управління розподілом прав доступу є імовірнісний показник довіри до користувача *P*(ProhibitedActions), що розраховується і постійно динамічно корегується з урахуванням статистики дій користувача мережі. Накопичувані статистичні дані з поділом даних щодо дій користувачів на коректні і некоректні з точки зору дотримання вимог політики безпеки роботи в мережі узагальнюються в моделі у формі матриць санкціонованих дій (MatrixOfAuthorizedActions) і заборонених дій (MatrixOfProhibitedActions).

Імовірнісний критерій довіри розраховується на основі накопичуваних статистичних даних про дії користувачів з інформаційними ресурсами мережі (даних матриць

MatrixOfAuthorizedActions і MatrixOfProhibitedActions) і узагальнюється для всіх користувачів в формі вектора критеріїв довіри VectorOfTrustCriteria.

Для реалізації динамічного управління правами доступу користувачів до ресурсів мережі використовуються рівні обмеження довірчого допуску до кожного інформаційного ресурсу, систематизовані у вигляді вектора граничних обмежень VectorOfBoundaryConstraints довірчого допуску до ресурсів мережі. Якщо відображувана вектором критеріїв довіри статистика дій певного користувача в полі інформаційних ресурсів мережі призводить до падіння рівня його довіри нижче за обмеження довірчого допуску до певного інформаційного ресурсу, то доступ відповідного користувача до цього ресурсу блокується.

Запропонована методика захисту інформаційних ресурсів мережі із застосуванням критеріїв довіри апробована для розмежування прав доступу в корпоративній мережі Хмельницького НУ і має перспективи подальшого застосування в системах інформаційної безпеки корпоративних мереж.

Список використаних джерел

1. Карпович І.М., Гладка О.М., Наконечна Ю.А. Аналіз ризиків безпеки інформаційної системи ІТ-підприємства. *Вчені записки ТНУ імені В.І. Вернадського. Серія: технічні науки*. 2020. Том 31 (70) № 5. С. 69-74.
2. Чинчик Д., Коробейнікова Т., Захарченко С. Методи та засоби комплексного захисту корпоративної мережі. *InterConf*. 2021. №84. С. 433-450.
3. Гапак О.М., Балога С.І. Захист інформації в комп'ютерних системах: підручник. Ужгород: Державний вищий навчальний заклад «Ужгородський НУ», 2021. 184 с.
4. Храпкін О.М. Захист інформаційно-комунікаційної мережі установи від несанкціонованого доступу. *Системи озброєння і військова техніка*. 2020. № 3(63). С.45-53.
5. Pienta D., Tams S., Bennet Thatcher J. Can Trust be Trusted in Cybersecurity? *Proceedings of the 53rd Hawaii International Conference on System Sciences*. 2020. P. 4264-4273

МАРТИНЮК А.І.,
Житомирський державний університет ім. І. Франка

БІБЛІОГРАФІЧНІ ПОСІБНИКИ В СИСТЕМІ ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ БІБЛІОТЕКИ ЖИТОМИРСЬКОГО ДЕРЖАВНОГО УНІВЕРСИТЕТУ ІМЕНІ ІВАНА ФРАНКА

Анотація: Здійснено огляд бібліографічних посібників, різноманітних за формами і жанрами, які пропонує віддаленим користувачам Бібліотека Житомирського державного університету імені Івана Франка.

Ключові слова: веб-сайт бібліотеки, електронний каталог, бібліографічні повідомлення, бібліографічні списки, віртуальні виставки.

Серед провідних освітянських бібліотек Житомирщини - Бібліотека Житомирського державного університету ім. І. Франка[1]. Як навчальний, науковий, інформаційний і культурно-просвітницький підрозділ університету, книгозбірня забезпечує високоякісне бібліотечно-бібліографічне та інформаційне обслуговування користувачів: студентів, аспірантів, викладачів, співробітників.

Одним із основних напрямів бібліотечного обслуговування Бібліотеки є створення власних бібліографічних посібників, що грунтується на використанні не тільки фонду книгозбірні, а й інформаційних ресурсів відкритого доступу.

Українськими бібліотекознавцями зроблено значний внесок в дослідження теоретичних і практичних питань створення і використання бібліографічних посібників. Змістові та жанрові особливості електронної бібліографічної продукції, яка створюється в бібліотеках

[1] Бібліотека Житомирського державного університету ім. І. Франка : веб-сайт. – Режим доступу: http://library.zu.edu.ua

УДК 004.056:004.942

МАЛИЦЬКИЙ ТАРАС
Хмельницький національний університет
e-mail: tarasmalitskyi@gmail.com
ЧЕШУН ВІКТОР
Хмельницький національний університет
https://orcid.org/0000-0002-3935-2068
e-mail: cheshunvn@khmnu.edu.ua
ЧЕШУН ОЛЕКСАНДР
Хмельницький національний університет
Sashacn228@gmail.com

МАТЕМАТИЧНА МОДЕЛЬ МЕТОДУ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ КОРПОРАТИВНОЇ МЕРЕЖІ ІЗ ЗАСТОСУВАННЯМ ІМОВІРНІСНИХ КРИТЕРІЇВ ДОВІРИ

Стаття присвячена презентації математичної моделі методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу із застосуванням імовірнісних критеріїв довіри. За результатами аналізу покладених на метод завдань, концептуально математичну модель методу захисту інформаційних ресурсів корпоративної мережі класифіковано як ймовірнісну статистичну модель систем управління доступом на основі концепції (критеріїв) довіри. Математична модель методу базується на аналізі взаємодії між різними суб'єктами (користувачами) та об'єктами (інформаційними ресурсами) в інформаційному середовищі корпоративної мережі та дає інструментарій для визначення ступеня довіри до суб'єктів інформаційних відносин в корпоративній мережі з точки зору інформаційної безпеки. Принципи застосування моделі продемонстровано структурно-логічною схемою взаємозв'язку елементів математичної моделі в реалізації методу.

Ключові слова: захист інформації, контроль доступу, корпоративна мережа, критерії довіри.

MALYTSKYI TARAS, CHESHUN VIKTOR, CHESHUN OLEKSANDR
Khmelnytsky National University

MATHEMATICAL MODEL OF THE METHOD OF PROTECTING CORPORATE NETWORK INFORMATION RESOURCES USING PROBABILITY TRUST CRITERIA

Abstract. The article is devoted to the presentation of a mathematical model of the method of protecting information resources of the corporate network from unauthorized access using probabilistic trust criteria. According to the results of the analysis of the tasks assigned to the method, the conceptual mathematical model of the method of protecting information resources of the corporate network is classified as a probabilistic statistical model of access control systems based on the concept (criteria) of trust. The mathematical model of the method is focused on the statistical analysis of the interaction between various subjects (users) and objects (information resources) in the information environment of the corporate network and provides a toolkit for determining the degree of trust in subjects of information relations in the corporate network from the point of view of information security.

Plural of objects and subjects of information relations are identified in the model. A binary access matrix was selected as the main element for managing access to information resources of the corporate network, the rules for its formation are detailed. A formula for calculating the probabilistic criterion of trust in the user based on statistical data about his actions in the network is also proposed. The principles of using the data of the vector of trust criteria and the vector of limit restrictions for making changes to the user's access rights are defined. The change of access rights is implemented in real time through the adjustment of the access matrix taking into account the decrease in the criterion of trust in the user according to the statistics of his work.

The principles of applying the model are demonstrated by the structural and logical diagram of the relationship between the elements of the mathematical model in the implementation of the method.

Keywords: information protection, access control, corporate network, trust criteria.

Вступ

Поширення цифрових технологій та нарощування їх можливостей супроводжується одночасним збільшенням кількості кіберзагроз. За таких умов ключовим аспектом сучасного бізнесу стає безпека корпоративних мереж як основної інфраструктури для забезпечення зв'язку і ефективної взаємодії між всіма рівнями організації, а також головного сховища комерційної та конфіденційної інформації.

Забезпечення ефективної безпеки корпоративних мереж вимагає комплексного підходу, який охоплює технологічні інновації та докладний аналіз потенційних загроз [1]. Технологічні інновації включають організаційні та програмно-апаратні заходи безпеки, такі як міжмережеві екрани, антивірусне програмне забезпечення, шифрування даних, аутентифікація та авторизація, навчання персоналу, регулярні оновлення та патчі, резервне копіювання та відновлення даних, а також моніторинг та аналіз активності мережі.

Одним із головних аспектів інформаційної безпеки корпоративних мереж є саме постійний моніторинг та аналіз активності мережі для блокування потенційно можливих шкідливих дій з інформаційними ресурсами [2]. Систематичний моніторинг мережі та виявлення загроз дозволяють не лише своєчасно реагувати на кібератаки та аномальну активність, але і запобігати можливим інцидентам кібербезпеки.

Постановка задачі

Ефективність заходів і засобів захисту інформаційних ресурсів корпоративних мереж полягає не тільки в можливості якнайшвидшого виявлення і блокування шкідливої активності користувачів, але й в прогнозуванні та попередженні можливих зловмисних дій. При цьому будь-яка оцінка потребує використання певних критеріїв.

В галузі інформаційної безпеки існує досить велика кількість національних і міжнародних стандартів, що пропонують різні підходи до вибору і застосування критеріїв оцінки безпеки інформаційних систем різних класів. До таких стандартів можна віднести: «Критерії оцінки довірених комп'ютерних систем Міністерства оборони» (TCSEC) [3,4], розроблені у США; Європейські стандарти під назвою «Критерії оцінки безпеки ІТ» (ITSEC) [5,6]; «Федеральні критерії» (FC) Германії [7,8]; «Канадські критерії безпеки комп'ютерних систем CTCPEC» [5,9]; «Загальні критерії оцінки безпеки інформаційних технологій» [10,11]; серії міжнародних стандартів ISO/IEC [12] тощо.

Міжнародні стандарти стали важливим еталоном оцінки безпеки інформаційних технологій та забезпечили загальноприйняті критерії для оцінки рівня захищеності ІТ-продуктів [13], але не надали універсальних критеріїв для всіх завдань кібербезпеки, що зумовило появу нових об'єктно-орієнтованих рішень.

В роботі [14] пропонується методика оцінювання ефективності системи інформаційної безпеки міністерства оборони та ЗСУ, яка грунтується на удосконаленій системі критеріїв та показників оцінювання ефективності функціонування системи забезпечення інформаційної безпеки. Автори методики оцінки захищеності інформаційних систем [15] пропонують здійснювати оцінку через розрахунок зв'язків, показників категорій та узагальненого показника, що беруть участь у оцінці, для надання рекомендацій щодо підвищення безпеки інформаційної системи.

Одним із перспективних напрямків оцінки захисту інформаційних ресурсів від несанкціонованого доступу, що активно розвивається, є використання в оцінці критеріїв довіри. Для прикладу, механізм оцінки аудиту SOC 2 [16] дозволяє виміряти ефективність функціонування системи безпеки компанії, спираючись на основні стандартів та Критеріїв довірених сервісів. Ці критерії дозволяють компанії визначити ступінь вірогідності, що процеси і системи відповідають встановленим нормам безпеки, конфіденційності, обробки, конфігурації та доступності даних.

Проведені дослідження свідчать про можливість застосування імовірнісних оцінок критеріїв довіри для захисту від несанкціонованого доступу інформаційних ресурсів корпоративної мережі. Для реалізації і апробації відповідної технології першочергово набуває актуальності задача вибору елементів математичної моделі.

Основна частина

Типовими сторонами, що вступають у взаємодію при реалізації систем управління доступом, є користувачі та інформаційні ресурси, ідентифіковані в Законі України «Про інформацію» [17] як суб'єкти і об'єкти інформаційних відносин. Для ідентифікації в математичній моделі суб'єктів і об'єктів інформаційних використано теорію множин:

$$\text{SUBJECTS}: \{\text{Subject}_1, \text{Subject}_2, \ldots, \text{Subject}_i, \ldots, \text{Subject}_k\}, \quad (1)$$

$$\text{OBJECTS}: \{\text{Object}_1, \text{Object}_2, \ldots, \text{Object}_j, \ldots, \text{Object}_n\}. \quad (2)$$

де SUBJECTS – множина, що відображує всіх користувачів корпоративної мережі $\text{Subject}_i \in \text{SUBJECTS}$, якими можуть бути як звичайні користувачі мережі з різними посадовими обов'язками (керівництво, посадові особи, оператори тощо), так і адміністратори цієї мережі; OBJECTS – множина, що відображує облікові об'єкти інформаційної взаємодії інформаційні ресурси корпоративної мережі $\text{Object}_j \in \text{OBJECTS}$, якими можуть бути бази даних, програмне забезпечення, файлові елементи, накопичувачі даних тощо.

Для відображення взаємодії об'єктів і суб'єктів інформаційних відносин найбільш інформативною і зручною в подальшій обробці є матрична форма представлення даних. З урахуванням приналежності математичної моделі методу до підкласу моделей систем управління доступом прийнято рішення обрати типовий для систем контролю доступу варіант представлення є даних у матричній формі – матрицю доступу [18]. Для зручності математичної обробки в моделі використано матрицю прав доступу булевого типу, в якій кожен елемент $AR_{ij} \in \text{MatrixOfAccessRights}$ є бінарним однорозрядним числом, що визначається за правилом:

$$AR_{ij} = \begin{cases} 0, & \text{якщо суб'єкт } \text{Subject}_i \in \text{SUBJECTS не має прав доступу до ресурсу } Object_j \in \text{OBJECTS}, \\ 1, & \text{якщо суб'єкт } \text{Subject}_i \in \text{SUBJECTS має права доступу до ресурсу } Object_j \in \text{OBJECTS}. \end{cases} \quad (3)$$

В узагальненому представлені матриця прав доступу множини користувачів корпоративної мережі SUBJECTS до множини облікованих інформаційних ресурсів корпоративної мережі OBJECTS має формат:

$$\text{MatrixOfAccessRights} = \begin{vmatrix} AR_{1,1} & AR_{1,2} & \cdots & AR_{1,|\text{OBJECTS}|} \\ AR_{2,1} & AR_{2,2} & \cdots & AR_{2,|\text{OBJECTS}|} \\ \vdots & \vdots & & \vdots \\ AR_{|\text{SUBJECTS}|,1} & AR_{|\text{SUBJECTS}|,2} & \cdots & AR_{|\text{SUBJECTS}|,|\text{OBJECTS}|} \end{vmatrix} \quad (4)$$

Наступний заявлений компонент моделі – матриця фіксації санкціонованих (дозволених) дій користувачів $\text{Subject}_i \in \text{SUBJECTS}$ корпоративної мережі в полі інформаційних ресурсів $\text{Object}_j \in \text{OBJECTS}$, яка в моделі ідентифікується як матриця санкціонованих дій MatrixOfAuthorizedActions з узагальненим представленням:

$$\text{MatrixOfAuthorizedActions} = \begin{vmatrix} AA_{1,1} & AA_{1,2} & \cdots & AA_{1,|\text{OBJECTS}|} \\ AA_{2,1} & AA_{2,2} & \cdots & AA_{2,|\text{OBJECTS}|} \\ \vdots & \vdots & & \vdots \\ AA_{|\text{SUBJECTS}|,1} & AA_{|\text{SUBJECTS}|,2} & \cdots & AA_{|\text{SUBJECTS}|,|\text{OBJECTS}|} \end{vmatrix} \quad (5)$$

Кожен елемент матриці санкціонованих дій $AA_{ij} \in$ MatrixOfAuthorizedActions, фактично, відіграє роль лічильника санкціонованих дій користувачів $\text{Subject}_i \in$ SUBJECTS корпоративної мережі в полі інформаційних ресурсів $\text{Object}_j \in$ OBJECTS (дій, які не порушують прав доступу користувачів до інформаційних ресурсів мережі).

Для фіксації спроб (вдалих або невдалих) здійснення несанкціонованих (заборонених) дій користувачів $\text{Subject}_i \in$ SUBJECTS корпоративної мережі в полі інформаційних ресурсів $\text{Object}_j \in$ OBJECTS в моделі використовується матриця заборонених дій MatrixOfProhibitedActions з узагальненим представленням:

$$\text{MatrixOfProhibitedActions} = \begin{vmatrix} PA_{1,1} & PA_{1,2} & \cdots & PA_{1,|OBJECTS|} \\ PA_{2,1} & PA_{2,2} & \cdots & PA_{2,|OBJECTS|} \\ \vdots & \vdots & & \vdots \\ PA_{|SUBJECTS|,1} & PA_{|SUBJECTS|,2} & \cdots & PA_{|SUBJECTS|,|OBJECTS|} \end{vmatrix} \quad (6)$$

Кожен елемент матриці заборонених дій $PA_{ij} \in$ MatrixOfProhibitedActions є лічильником спроб доступу до інформаційного ресурсу $\text{Object}_j \in$ OBJECTS, які порушують надані користувачу $\text{Subject}_i \in$ SUBJECTS права.

Матриці санкціонованих дій MatrixOfAuthorizedActions і заборонених дій MatrixOfProhibitedActions відображають задекларовану в концептуальних положеннях методу приналежність математичної моделі до різновидів статистичних моделей, оскільки вони мають використовуватись для аналізу випадкових процесів та подій у корпоративній мережі, пов'язаних з поведінкою користувачів $\text{Subject}_i \in$ SUBJECTS, яку апріорно неможливо передбачити. В даній інтерпретації математичної моделі як лічильники накопичення будуть працювати лише елементи $AA_{ij} \in$ MatrixOfAuthorizedActions, для яких $AR_{ij}=1$, тобто, робота користувача з ресурсами, до яких йому надано права доступу. Як лічильники накопичення заборонених дій будуть працювати елементи $PA_{ij} \in$ MatrixOfProhibitedActions, для яких $AR_{ij}=0$, тобто, дії користувача з ресурсами, до яких йому заборонено доступ.

Наступним кроком деталізуємо в математичній моделі задекларовану в ймовірнісну статистичну складову, якою передбачається використання ймовірнісні підходів прогнозування-попередження зловмисних дій та статистичних методів аналізу поведінки користувачів. Перехід від статистичних даних до імовірнісних оцінок будемо виконувати традиційними для таких задач способами через розрахунок $\text{Subject}_i \in$ SUBJECTS співвідношення санкціонованих дій кожного користувача $\text{Subject}_i \in$ SUBJECTS до його загальної активності:

$$P(\text{AuthorizedActions})_i = \sum_{\forall (AA_{ij}+PA_{ij})>0}^{|OBJECTS|} \frac{AA_{ij}}{AA_{ij}+PA_{ij}}, \quad (7)$$

де $P(\text{AuthorizedActions})_i$ – статистична імовірність роботи користувача $\text{Subject}_i \in$ SUBJECTS без несанкціонованих дій в полі OBJECTS інформаційних ресурсів корпоративної мережі. Обмеження $\forall (AA_{ij}+PA_{ij})>0$ в формулу (7) введене через можливу нульову статистичну активність користувачів, які з різних причин ще не працювали в мережі (новозарахованих користувачів тощо), що враховується при обчисленні статистичної імовірності санкціонованих дій $P(\text{AuthorizedActions})_i$ для уникнення ситуації з діленням на нуль.

Статистична імовірність коректності дій користувача $\text{Subject}_i \in$ SUBJECTS в полі OBJECTS інформаційних ресурсів корпоративної мережі передбачається до використання як основний критерій довіри для захисту

інформаційних ресурсів корпоративної мережі від несанкціонованого доступу. Для більш наочного представлення розраховувані за формулою (7) значення групуються у вигляді вектора критеріїв довіри VectorOfTrustCriteria:

$$\text{VectorOfTrustCriteria} = \begin{vmatrix} P(\text{AuthorizedActions})_1 \\ P(\text{AuthorizedActions})_2 \\ \vdots \\ P(\text{AuthorizedActions})_{|\text{SUBJECTS}|} \end{vmatrix}. \quad (8)$$

Обмеження для блокування прав доступу користувачів $\text{Subject}_i \in \text{SUBJECTS}$ за критерієм довіри до кожного облікованого інформаційного ресурсу $\text{Object}_j \in \text{OBJECTS}$ в моделі представлені як вектор граничних обмежень VectorOfBoundaryConstraints:

$$\text{VectorOfBoundaryConstraints} = \begin{vmatrix} BC_1 \\ BC_2 \\ \vdots \\ BC_{|\text{OBJECTS}|} \end{vmatrix}, \quad (9)$$

де BC_j – рівень обмеження довірчого допуску користувачів $\text{Subject}_i \in \text{SUBJECTS}$ до ресурсу $\text{Object}_j \in \text{OBJECTS}$.

На рисунку 1 представлена структурно-логічна схема взаємозв'язку елементів математичної моделі в реалізації захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри.

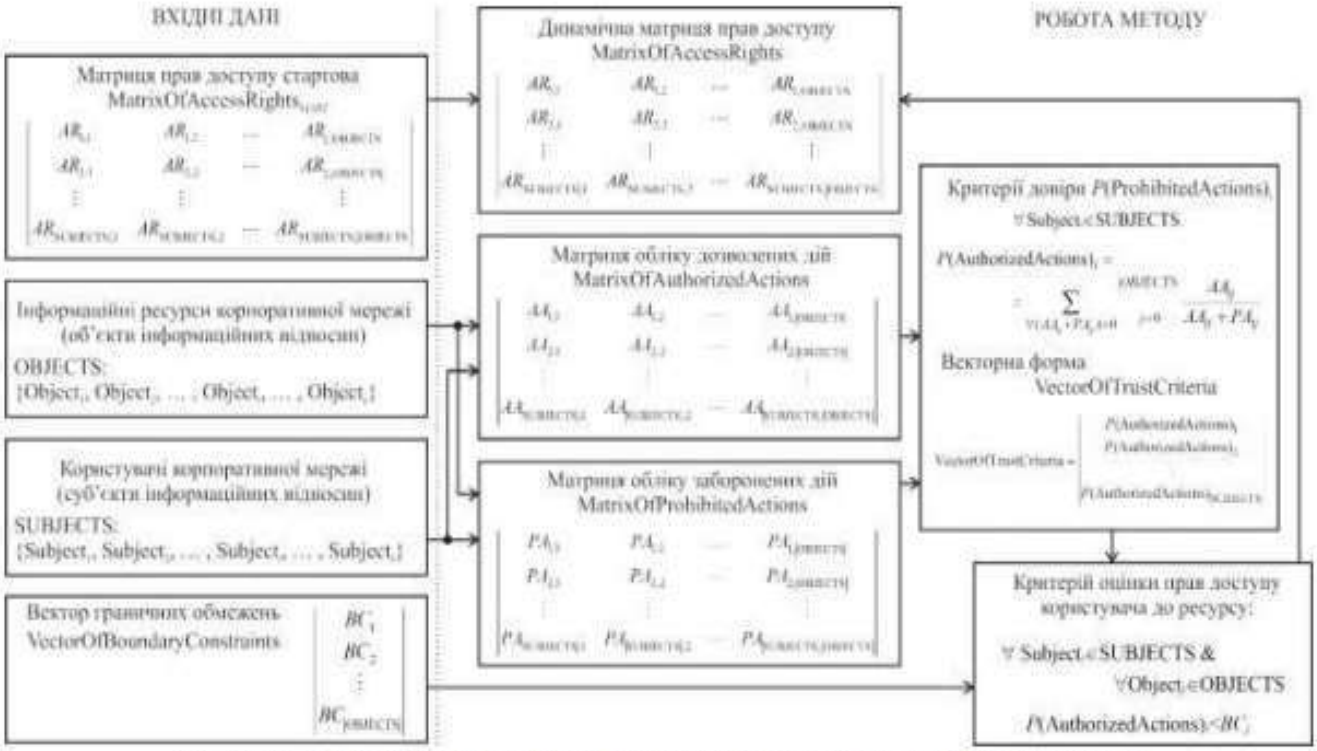


Рис. 1 – Структурно-логічна схема взаємозв'язку складових математичної моделі в реалізації методу

Основою для корегування прав доступу є рівень обмеження довірчого допуску $BC_j \in$ VectorOfBoundaryConstraints користувачів SUBJECTS до ресурсу $Object_j \in$ OBJECTS і значення імовірнісної критерія оцінки довіри $P(\text{AuthorizedActions})_i$ до користувача $Subject_i \in$ SUBJECTS. Після зменшення рівня довіри до користувача нижче за рівень обмеження довірчого допуску $P(\text{AuthorizedActions})_i < BC_j$, доступ до ресурсу $Object_j \in$ OBJECTS користувачу $Subject_i \in$ SUBJECTS автоматично блокується до прийняття рішення щодо подальших заходів комісією (експертами) з розслідування інцидентів інформаційної безпеки

Висновки

В статті презентовано математичну модель методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу із застосуванням імовірнісних критеріїв довіри. Математична модель методу базується на аналізі взаємодії між різними суб'єктами (користувачами) та об'єктами (інформаційними ресурсами) в інформаційному середовищі корпоративної мережі та дає інструментарій для визначення ступеня довіри до суб'єктів інформаційних відносин в корпоративній мережі з точки зору інформаційної безпеки. В якості критерію довіри до суб'єктів взаємодії в інформаційному просторі корпоративної мережі використовується імовірнісний показник, що формується на основі накопичуваної статистики попередньої діяльності кожного суб'єкта із урахуванням зафіксованих випадків шкідливої активності відносно загального показника активності.

Математичну модель методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу ідентифіковано як ймовірнісну статистичну модель систем управління доступом на основі концепції (критеріїв) довіри.

Література

1. Карпович І.М., Гладка О.М., Наконечна Ю.А. Аналіз ризиків безпеки інформаційної системи ІТ-підприємства. *Вчені записки ТНУ імені В.І. Вернадського. Серія: технічні науки.* 2020. Том 31 (70) № 5. С. 69-74.

2. Храпкін О.М. Захист інформаційно-комунікаційної мережі установи від несанкціонованого доступу. *Системи озброєння і військова техніка*. 2020. № 3(63). С.45-53.

3. Livshitz I.I., Neklyudov A.V., Lontsikh P.A. Evaluation of IT security – genesis and its state-of-art. *International Conference Information Technologies in Business and Industry* 2018. IOP Publishing. 2018. С. 1-7.

4. Lawrence C. Miller and Peter H. Gregory. Evaluation Criteria of Systems Security Controls. *CISSP Articles*. 2018. URL: https://www.dummies.com/article/academics-the-arts/study-skills-test-prep/cissp/evaluation-criteria-systems-security-controls-254878/ (дата звернення: 30.11.2023).

5. Abhi G. CISSP Concepts – Trusted Computing Base/ TCEC, ITSEC and Common Criteria. *Cyber Management Alliance Articles*. Jan 28, 2020. URL: https://www.cm-alliance.com/cissp/trusted-computing-base/-tcec-itsec-and-common-criteria (дата звернення: 30.11.2023).

6. Randal Allen. Evolved Artificial Intelligence for Stochastic Clustering Unsupervised Learning. *Interservice/Industry Training, Simulation, and Education Conference*. 2020. Paper № 20258. 8 p.

7. Donald P. Kommersio The Basic Law: A Fifty Year Assessment. *German Law Journal*. 2019. Volume 20, Issue 4. P. 571-582.

8. Турчак А. Основні складові інформаційної безпеки держави. *Аспекти публічного управління*. Том 7, № 5. 2019. С. 44-56.

9. The Canadian Trusted Computer Product Evaluation Criteria 3rd Ed. CTCPEC Version 3.0e. Publisher: Communications Security Establishment, 1993. Last modified: April 15, 2022. 208 p.

10. Defining Security Requirements with the Common Criteria: Applications, Adoptions, and Challenges / Nan Sun et al. *Computer Science - Cryptography and Security*. 2022. V.1. P. 44756-44777.

11. A survey on common criteria (CC) evaluating schemes for security assessment of IT products / Chang-Tsun Li et al. PeerJ Comput Sci. 2021. №7. 22p.

12. Standards. URL:https://www.iso.org/standards.html (дата звернення: 30.11.2023).

13. Дикий О. В., Флюнт М. О. Стандарти інформаційної безпеки: компаративне дослідження. *Право та державне управління*. 2019. № 2 (35), том 1. С. 80-87.

14. Петренко К.М. Удосконалена методика оцінювання ефективності системи забезпечення інформаційної безпеки Міністерства оборони та збройних сил України. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2022. № 3 (45). С. 97-100.

15. Батечко С.В., Лебедєва О.Ю., Зоріло В.В. Методика оцінки захищеності інформаційних систем. *Інформатика та математичні методи в моделюванні*. 2021. Том 11, № 3. С. 173-180.

16. Kim Koch. How to Comply with Trust Services Criteria for SOC 2 Examinations. *Moss Adams*. 2022. URL: https://www.mossadams.com/articles/2021/07/soc-2-trust-services-criteria (дата звернення: 5.12.2023).

17. Про інформацію : Закон України від 2.10.1992р. № № 2657-XII : Редакція від 27.07.2023р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#doc_info (дата звернення: 11.10.2023).

18. Марченко П. А. Методи розмежування доступу в розподілених системах кешування даних. Магістерська дисертація. Київ: НТУ УКРАЇНИ «КПІ ім. І. Сікорського», 2018. 91 с.

References

1. Karpovych I.M., Hladka O.M., Nakonechna Yu.A. Analiz ryzykiv bezpeky informatsiinoi systemy IT-pidpryiemstva. *Vcheni zapysky TNU imeni V.I. Vernadskoho. Seriia: tekhnichni nauky*. 2020. Tom 31 (70) № 5. C. 69-74.

2. Khrapkin O.M. Zakhyst informatsiino-komunikatsiinoi merezhi ustanovy vid nesanktsionovanoho dostupu. *Systemy ozbroiennia i vitskova tekhnika*. 2020. № 3(63). S.45-53.

3. Livshitz I.I., Neklyudov A.V., Lontsikh P.A. Evaluation of IT security – genesis and its state-of-art. International *Conference Information Technologies in Business and Industry* 2018. IOP Publishing. 2018. C. 1-7.

4. Lawrence C. Miller and Peter H. Gregory. Evaluation Criteria of Systems Security Controls. *CISSP Articles*. 2018. URL: https://www.dummies.com/article/academics-the-arts/study-skills-test-prep/cissp/evaluation-criteria-systems-security-controls-254878/ (date of access: 30.09.2023).

5. Abhi G. CISSP Concepts – Trusted Computing Base/ TCEC, ITSEC and Common Criteria. *Cyber Management Alliance Articles*. Jan 28, 2020. URL: https://www.cm-alliance.com/cissp/trusted-computing-base/-tcec-itsec-and-common-criteria (date of access: 30.09.2023).

6. Randal Allen. Evolved Artificial Intelligence for Stochastic Clustering Unsupervised Learning. *Interservice/Industry Training, Simulation, and Education Conference*. 2020. Paper № 20258. 8 p.

7. Donald P. Kommersio The Basic Law: A Fifty Year Assessment. *German Law Journal*. 2019. Volume 20, Issue 4. P. 571-582.

8. Turchak A. Osnovni skladovi informatsiinoi bezpeky derzhavy. *Aspekty publichnoho upravlinnia*. Tom 7, № 5. 2019. S. 44-56.

9. The Canadian Trusted Computer Product Evaluation Criteria 3rd Ed. CTCPEC Version 3.0e. Publisher: Communications Security Establishment, 1993. Last modified: April 15, 2022. 208 p.

10. Defining Security Requirements with the Common Criteria: Applications, Adoptions, and Challenges / Nan Sun et al. *Computer Science - Cryptography and Security*. 2022. V.1. P. 44756-44777.

11. A survey on common criteria (CC) evaluating schemes for security assessment of IT products / Chang-Tsun Li et al. *PeerJ Comput Sci*. 2021. №7. 22p.

12. Standards. URL:https://www.iso.org/standards.html (date of access: 30.11.2023).

13. Dykyi O. V., Fliunt M. O. Standarty informatsiinoi bezpeky: komparatyvne doslidzhennia. *Pravo ta derzhavne upravlinnia*. 2019. № 2 (35), tom 1. S. 80-87.

14. Petrenko K.M. Udoskonalena metodyka otsiniuvannia efektyvnosti systemy zabezpechennia informatsiinoi bezpeky Ministerstva oborony ta zbroinykh syl Ukrainy. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*. 2022. № 3 (45). S. 97-100.

15. Batechko S.V., Lebedieva O.Iu., Zorilo V.V. Metodyka otsinky zakhyshchenosti informatsiinykh system. *Informatyka ta matematychni metody v modeliuvanni*. 2021. Tom 11, № 3. S. 173-180.

16. Kim Koch. How to Comply with Trust Services Criteria for SOC 2 Examinations. *Moss Adams*. 2022. URL: https://www.mossadams.com/articles/2021/07/soc-2-trust-services-criteria (date of access: 5.12.2023).

17. Marchenko P. A. Metody rozmezhuvannia dostupu v rozpodilenykh systemakh keshuvannia danykh. Mahisterska dysertatsiia. Kyiv: NTU UKRAINY «KPI im. I. Sikorskoho», 2018. 91 s.

ДОДАТОК Б

Презентація кваліфікаційної роботи

Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

Малицький Тарас Борисович

Метод захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри

спеціальність 125 – Кібербезпека

Науковий керівник: к.т.н., доцент **Чешун Віктор Миколайович**

ЗАГАЛЬНА ХАРАКТЕРИСТИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ МАГІСТРА

Мета кваліфікаційної роботи полягає у вдосконаленні технологій захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу за рахунок оцінки імовірності виникнення загроз і попередження несанкціонованих дій користувачів на основі накопичуваних статистичних даних.

Об'єктом дослідження є процес управління доступом користувачів до інформаційних ресурсів корпоративної мережі.

Предметом дослідження є методи і моделі динамічного адаптивного управління правами доступу користувачів до інформаційних ресурсів корпоративної мережі на основі статистичних даних.

Наукова новизна отриманих результатів:

1. Запропоновано оригінальну концепцію реалізації методу захисту інформаційних ресурсів корпоративної мережі в термінах математичної моделі;
2. Запропоновано спосіб формування на основі накопичуваних статистичних даних імовірнісних показників критеріїв довіри і їх використання для динамічного адаптивного управління правами доступу користувачів до інформаційних ресурсів корпоративної мережі.

Практична значимість отриманих результатів полягає у визначенні положень і розробці алгоритмів методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу, який забезпечує зменшення загроз від дій користувачів із зафіксованими порушеннями політики безпеки роботи в мережі.

Задачі досліджень у роботі формулюються наступним чином:

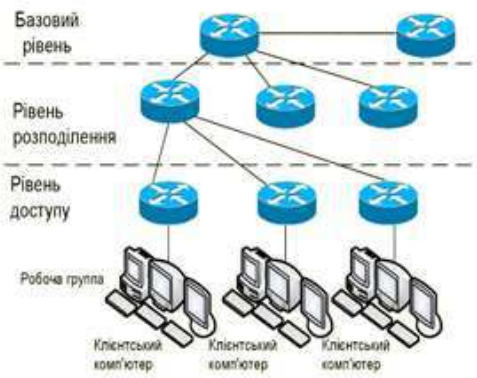
- виявити перспективні напрямки та способи вдосконалення захисту інформаційних ресурсів корпоративної мережі на основі статистичних даних про дії користувачів;
- визначити основні положення методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри;
- розробити математичну модель методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри;
- розробити алгоритми реалізації методу;
- здійснити апробацію запропонованих теоретичних і алгоритмічних рішень.

В основі методів дослідження лежать положеннях інформаційної безпеки, теорії аутентифікації і управління доступом, теорії ймовірностей і математичної статистики, теорії множин.

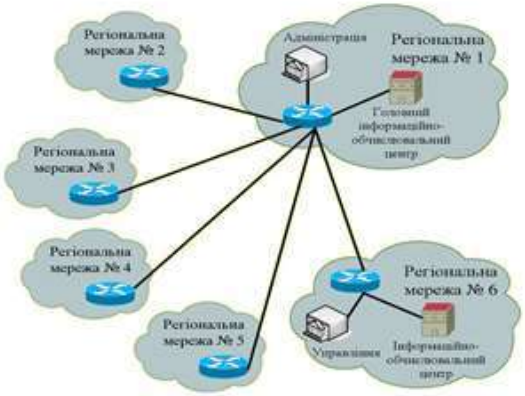
Апробація роботи. Наукові результати і основні положення магістерської роботи доповідались і обговорювались на Всеукраїнській і 2-х міжнародних науково-практичних конференціях.

Публікації. За темою магістерської роботи опубліковано тези доповідей на Всеукраїнській та 2-х міжнародних науково-практичних конференціях.

КОРПОРАТИВНІ МЕРЕЖІ ЯК ОБ'ЄКТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ



Трирівнева ієрархічна модель корпоративної мережі



Модель розподіленої корпоративної мережі

Висновок 1 : Корпоративні мережі можуть мати різну організацію, але для них є характерними: розподілена інфраструктура, централізоване управління, загальні ресурси, обмежене коло користувачів (співробітники).

Висновок 2 : Основними типами загроз інформаційним ресурсам корпоративної мережі є внутрішні.

Висновок 3 : Управління доступом до інформаційних ресурсів на основі імовірнісних оцінок критеріїв довіри до користувачів є перспективним напрямком у вдосконаленні технологій захисту зазначених ресурсів.

Перший науковий результат: **МАТЕМАТИЧНА МОДЕЛЬ МЕТОДУ**

Базові елементи моделі

SUBJECTS:{Subject$_1$, Subject$_2$, … , Subject$_i$, … , Subject$_k$} – **множина ідентифікаторів суб'єктів інформаційних відносин**

OBJECTS:{Object$_1$, Object$_2$, … , Object$_j$, … , Object$_n$} – **множина ідентифікаторів об'єктів інформаційних відносин**

Матриця прав доступу:

$$MatrixOfAccessRights = \begin{vmatrix} AR_{11} & AR_{12} & \cdots & AR_{1|OBJECTS|} \\ AR_{21} & AR_{22} & \cdots & AR_{2|OBJECTS|} \\ \vdots & \vdots & & \vdots \\ AR_{|SUBJECTS|1} & AR_{|SUBJECTS|2} & \cdots & AR_{|SUBJECTS||OBJECTS|} \end{vmatrix}$$

Правило визначення елементів матриці:

$$AR_{ij} = \begin{cases} 0, & \text{якщо суб'єкт } Subject_i \in SUBJECTS \text{ не має} \\ & \text{прав доступу до ресурсу } Object_j \in OBJECTS, \\ 1, & \text{якщо суб'єкт } Subject_i \in SUBJECTS \text{ має} \\ & \text{права доступу до ресурсу } Object_j \in OBJECTS,. \end{cases}$$

Вектор граничних обмежень прав доступу до ресурсів:

$$VectorOfBoundaryConstraints = \begin{vmatrix} BC_1 \\ BC_2 \\ \vdots \\ BC_{|OBJECTS|} \end{vmatrix}$$

Статистичні (імовірнісні) елементи моделі

Матриця санкціонованих (коректних) дій:

$$MatrixOfAuthorizedActions = \begin{vmatrix} AA_{11} & AA_{12} & \cdots & AA_{1|OBJECTS|} \\ AA_{21} & AA_{22} & \cdots & AA_{2|OBJECTS|} \\ \vdots & \vdots & & \vdots \\ AA_{|SUBJECTS|1} & AA_{|SUBJECTS|2} & \cdots & AA_{|SUBJECTS||OBJECTS|} \end{vmatrix}$$

Матриця заборонених дій (порушень):

$$MatrixOfProhibitedActions = \begin{vmatrix} PA_{11} & PA_{12} & \cdots & PA_{1|OBJECTS|} \\ PA_{21} & PA_{22} & \cdots & PA_{2|OBJECTS|} \\ \vdots & \vdots & & \vdots \\ PA_{|SUBJECTS|1} & PA_{|SUBJECTS|2} & \cdots & PA_{|SUBJECTS||OBJECTS|} \end{vmatrix}$$

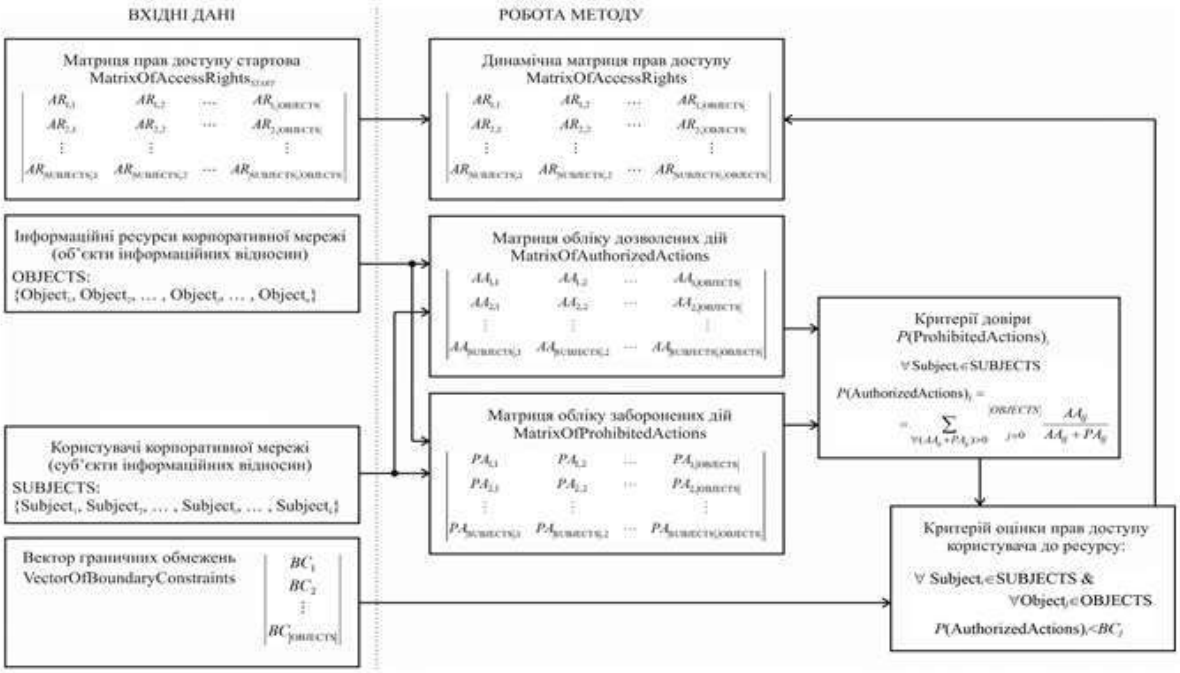
Критерій довіри - статистична імовірність коректних дій:

$$P(AuthorizedActions)_i = \sum_{\forall (AA_{ij}+PA_{ij})>0}^{|OBJECTS|} \frac{AA_{ij}}{AA_{ij}+PA_{ij}}$$

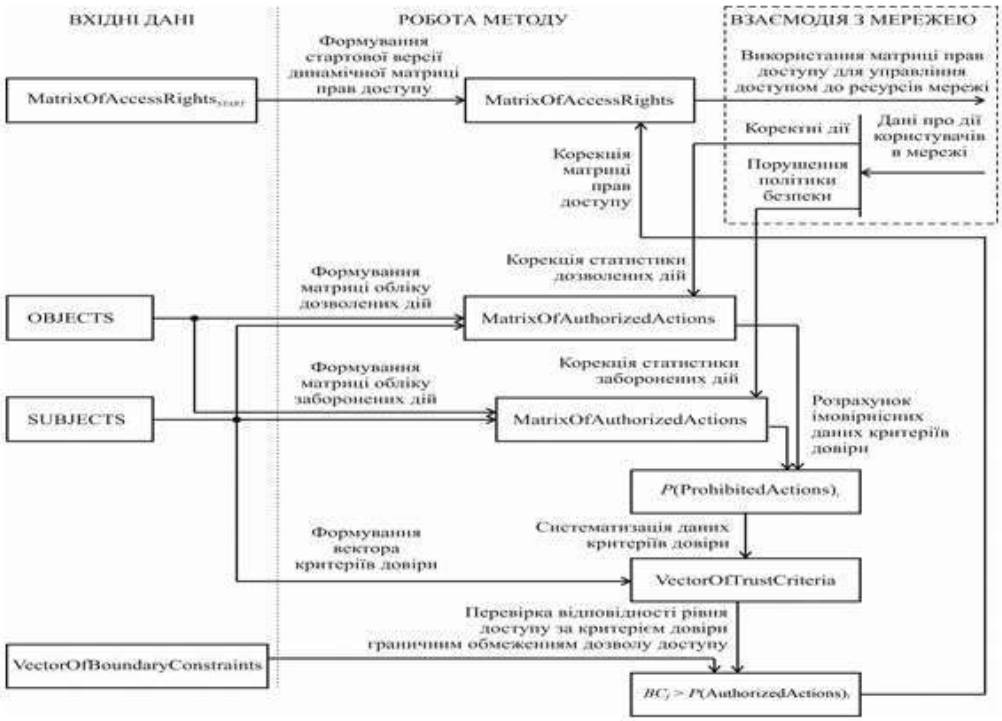
Вектор критеріїв довіри:

$$VectorOfTrustCriteria = \begin{vmatrix} P(AuthorizedActions)_1 \\ P(AuthorizedActions)_2 \\ \vdots \\ P(AuthorizedActions)_{|SUBJECTS|} \end{vmatrix}$$

Перший науковий результат **СТРУКТУРНО-ЛОГІЧНА СХЕМА РАЛІЗАЦІЇ КОНЦЕПЦІЇ МЕТОДУ В ТЕРМІНАХ МАТЕМАТИЧНОЇ МОДЕЛІ**



Перший науковий результат **ПРИЧИННО-НАСЛІДКОВА СХЕМА РЕАЛІЗАЦІЇ КОНЦЕПЦІЇ МЕТОДУ В ТЕРМІНАХ МАТЕМАТИЧНОЇ МОДЕЛІ**



Другий науковий результат

Основні положення методу

- Метод розробляється для підвищення ефективності захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу.
- Математичною основою методу є запропонована ймовірнісна статистична математична модель управління доступом на основі концепції (критеріїв) довіри.
- Метод базується на статистичному аналізі дій користувачів і обмеженні прав доступу при виявленні порушень користувачем вимог політики безпеки роботи в мережі.
- Реагування на порушення користувачем політики безпеки з прийняттям рішення щодо обмеження прав доступу здійснюється автоматично в реальному масштабі часу.
- Базовим критерієм для динамічного управління розподілом прав доступу є імовірнісний критерій довіри, що розраховується і постійно динамічно корегується з урахуванням дій користувача в мережі.

Другий науковий результат

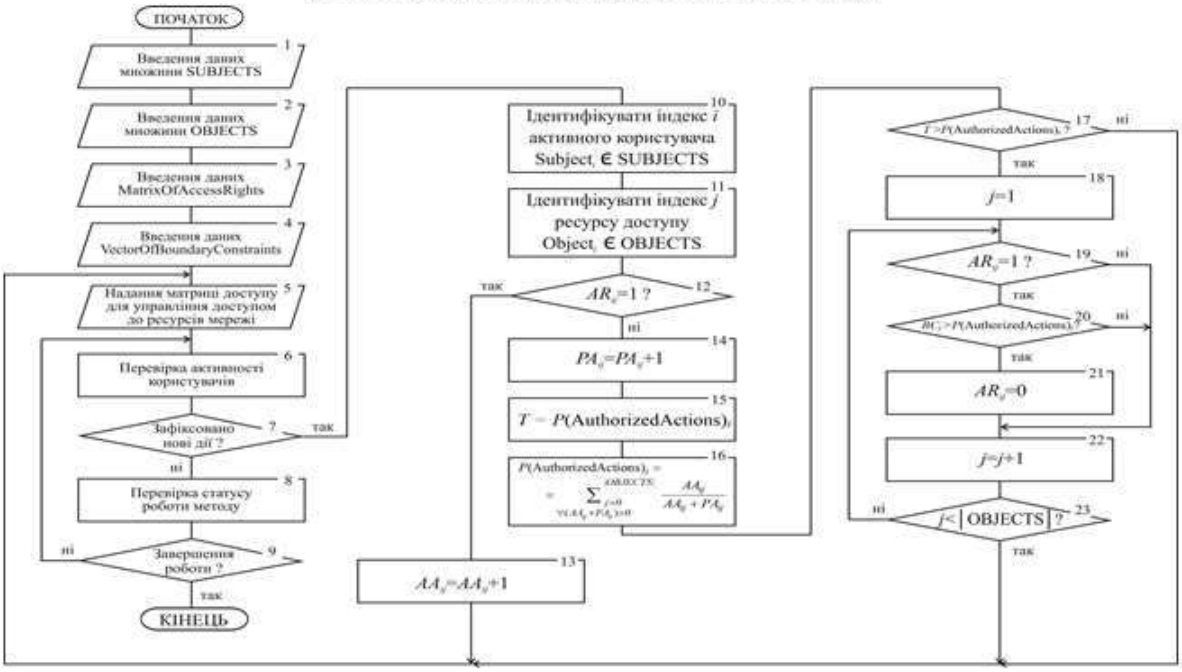
АЛГОРИТМІЧНА РЕАЛІЗАЦІЯ МЕТОДУ

Узагальнений алгоритм реалізації методу

Другий науковий результат

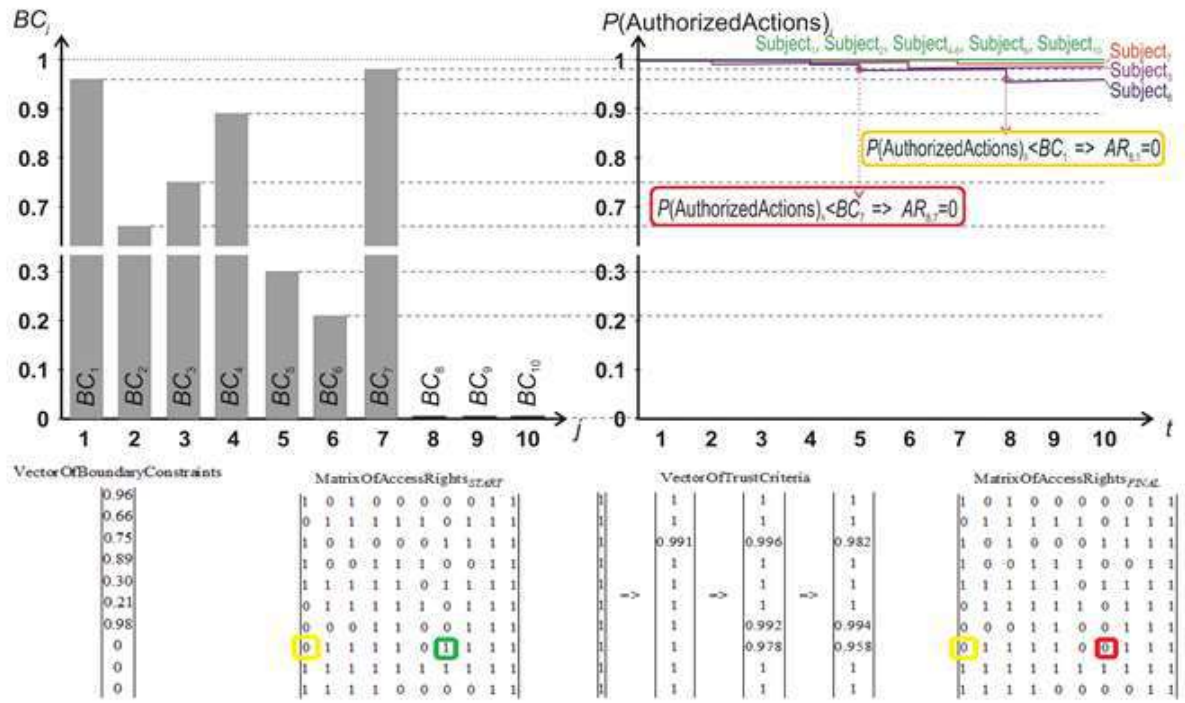
АЛГОРИТМІЧНА РЕАЛІЗАЦІЯ МЕТОДУ

Деталізований алгоритм реалізації методу



АПРОБАЦІЯ МЕТОДУ

Діаграма граничних обмежень прав доступу до ресурсів **Динаміка зміни критеріїв довіри**



ВИСНОВКИ

В роботі за результатами теоретичних та практичних досліджень виконано розробку методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри. При розробці методу переслідувалась мета, що полягає у вдосконаленні технологій захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу за рахунок оцінки імовірності виникнення загроз і попередження несанкціонованих дій користувачів на основі накопичуваних статистичних даних.

Для реалізації програми досліджень виконано наступні роботи:

- проведене дослідження корпоративних мереж як об'єкту інформаційної безпеки, в ході якого були досліджені принципи організації корпоративних мереж та типові загрози безпеці інформаційних ресурсів і виявлено перспективні напрямки та способи вдосконалення захисту інформаційних ресурсів корпоративної мережі на основі статистичних даних про дії користувачів;
- визначено основні положення методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри;
- розроблено математичну модель методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри, запропоновано оригінальну концепцію реалізації методу в термінах математичної моделі;
- розроблено узагальнений і деталізований алгоритми реалізації методу;
- здійснено апробацію дієвості прийнятих теоретичних і алгоритмічних рішень методу.

Оцінка отриманих результатів дозволила дійти загального висновку, що в роботі виконані всі поставлені задання і досягнуто загальної мети дослідження.

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Малицького Тараса Борисовича
ПІБ здобувача вищої освіти

Студента ФІТ, 2 курсу, групи КБм-22-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у хмельницькому національному університеті» від 31.08.2023, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

5.12.2023
дата

підпис

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1015978952

Дата перевірки:
07.12.2023 09:54:58 EET

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
07.12.2023 09:55:43 EET

ID користувача:
100008300

Назва документа: **Малицький на плагіат**

Кількість сторінок: **77** Кількість слів: **13502** Кількість символів: **110988** Розмір файлу: **1,002.88 KB** ID файлу: **1015658984**

3.38%
Схожість

Найбільша схожість: **1.07%** з Інтернет-джерелом (http://logic-bratsk.ru/radio/tech_lib/elektron/Indikatr.doc)

2.87% Джерела з Інтернету	341	Сторінка 79
2.06% Джерела з Бібліотеки	95	Сторінка 80

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 1.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 9%**

ID: 121982 Назва: Метод захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри Додано в БД: 2023-12-07 Автора: Малицький Т.Б. Керівники: Чешун В.М. Консультанти: Опоненти:	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
	95682	1294	1018 (1%)	15 (1%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:
Назва: Метод захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри

Автор: Малицький Тарас Борисович

Спеціальність: 125 – Кібербезпека

Освітня програма: освітньо-професійна

Науковий керівник: Чешун Віктор Миколайович, к.т.н, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 96,62%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 99%.

Згідно з правилами чинного Положення «Про систему забезпечення академічної доброчесності у хмельницькому національному університеті» від 31.08.2023, авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 90-100 %, визнається роботою з високою унікальністю тексту і допускається до захисту.

Керівник роботи _____ В.М. Чешун

Гарант ОП _____ В.Ю. Тітова

Завідувач кафедри кібербезпеки _____ Ю.П. Кльоц

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «магістр»

Студент Малицький Тарас Борисович

Тема Метод захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «магістр»:

кількість листів креслень - ; кількість сторінок записки 83

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі запропоновано метод захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри. Робота включає в себе математичну модель, основні положення та загальну концепцію методу, реалізацію концепції в термінах математичної моделі, узагальнений і деталізований алгоритми реалізації методу, а також презентацію та апробацію роботи методу

2. Висновок про відповідність кваліфікаційної роботи завданню Кваліфікаційна робота відповідає поставленому завданню як в теоретичній, так і в практичній частині

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі подана загальна характеристика поставленої задачі, чітко визначено об'єкт, предмет та методи дослідження, сформульована актуальність; визначені задачі, які необхідно вирішити для досягнення поставленої мети, практична цінність отриманих результатів, їхня новизна та наведені відомості про публікації. У першому розділі проведене дослідження технологій і методів захисту інформаційних ресурсів корпоративної мережі, виконане обґрунтування актуальності теми дослідження і зроблена постановка задачі.. В другому розділі запропоновано математичну модель методу. В третьому розділі роботи презентовано сам метод захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри - визначено концепцію методу як базову теоретичну основу, сформульована концепція методу, представлено структурно-логічну і причинно-наслідкову схеми реалізації концепції методу в термінах математичної моделі, запропоновано алгоритмічну реалізацію методу. В четвертому розділі здійснене дослідження актуальних загроз безпеці інформаційних ресурсів корпоративної мережі і можливостей запропонованого методу щодо протидії виявленим загрозам та проведена експериментальна апробація методу.

4. Позитивні сторони роботи Кваліфікаційна робота має комплексну наукову і практичну цінність. Наукова цінність полягає у пропозиції способу оцінки імовірнісних показників критеріїв довіри і їх використання для динамічного адаптивного управління правами доступу користувачів до інформаційних ресурсів корпоративної мережі та в оригінальній концепції реалізації методу захисту інформаційних ресурсів корпоративної мережі в термінах математичної моделі. Практична цінність полягає у можливості застосування методу та алгоритмів його реалізації для підвищення ефективності захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу.

5. Негативні сторони роботи В роботі не розглянуте питання можливостей застосування методу для протидії зовнішнім загрозам корпоративної мережі

6. Оцінка графічного оформлення та пояснювальної записки роботи Оформлення всіх матеріалів кваліфікаційної роботи є якісним, здійснене з дотриманням актуальних стандартів та інституційних положень ХНУ. Пояснювальна записка відповідає нормам щодо її оформлення як за структурою, так і за представленням і форматуванням матеріалу.

7. Відгук про роботу в цілому Кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та наскрізно пов'язаний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. Презентаційний та ілюстративний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої мети.

8. Інші зауваження Окремі описи в пояснювальній записці подано занадто деталізовано, що ускладнює сприйняття матеріалу фахівцями в обраній предметній галузі

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінку «відмінно».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
Підченко Сергій Костянтинович
Завідувач кафедри ТМІТ, доктор технічних наук, професор

« 7 » 12 2023. _____ (підпис)