МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

На правах рукопису

Суліма Олександр Андрійович

УДК 004.056.52

МЕТОДИ ОРГАНІЗАЦІЇ ЗАХИСТУ ДОСТУПУ ДО ІНФОРМАЦІЙНИХ СИСТЕМ НА ОСНОВІ ВИКОРИСТАННЯ БАГАТОРІВНЕВИХ МОДЕЛЕЙ

Спеціальність 05.13.21 - системи захисту інформації

Дисертація на здобуття наукового ступеня кандидата технічних наук

Науковий керівник:
Давиденко Анатолій Миколайович
кандидат технічних наук

Київ — 2017

ЗМІСТ

АНОТАЦІЯ

Суліма О.А. Методи організації захисту доступу до інформаційних систем на основі використання багаторівневих моделей. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук виконана в Інституті проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України за спеціальністю 05.13.21 «Системи захисту інформації». – Національний авіаційний університет. Київ, 2017.

Актуальність дисертаційної роботи Суліми О.А. обумовлена важливістю розв’язання завдань щодо підвищення рівня захисту інформаційних систем від несанкціонованого доступу до їх даних.

Мета дослідження полягає у вирішенні науково-прикладної задачі побудови інформаційних засобів захисту даних в інформаційних системах на основі використання багаторівневої системи надання повноважень користувачам. Для досягнення поставленої мети здобувачем розв'язано наступні задачі: розроблено методи оцінки рівня повноважень на використання даних різних рівнів їх конфіденційності; розроблено базові елементи для практичного запровадження дворівневої системи надання повноважень на використання даних користувачами; розроблено методи оцінки параметрів інформаційних елементів та параметрів інформаційного запиту прикладних задач, для розв'язання яких необхідні дані, що знаходяться в інформаційній системі; розроблено компоненти дворівневої системи з надання повноважень користувачам на використання даних.

Наукова новизна отриманих результатів полягає у наступному: вперше розроблено метод визначення параметрів інформаційних запитів прикладних задач, що дозволило розширити аналіз умов, які визначають можливість надання повноважень прикладній задачі на використання даних; уперше розроблено дворівневу модель надання повноважень на використання даних користувачами, які звертаються за ними до інформаційної системи; вперше розроблено основні компоненти дворівневої моделі доступу до даних; уперше запропоновано

застосування розподілу рівнів доступу до даних, залежно від ступеня їх конфіденційності, які функціонують незалежно один від одного.

Особистий внесок здобувача полягає у тому, що автор самостійно отримав основні результати роботи, які підтверджуються особистими публікаціями в наукових виданнях та практичним застосуванням.

Структура дисертаційної роботи складається із вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. Робота викладена на 193 сторінках і містить 164 сторінки основного тексту.

У першому розділі проаналізовано загальновідомі методи надання повноважень користувачам на використання даних, за якими вони звертаються до інформаційної системи. Найбільш поширеною моделлю надання повноважень є матрична модель доступу до даних. Така модель передбачає можливість надання різного типу повноважень на використання даних. Прикладом таких повноважень є: повноваження на зчитування даних; повноваження на запис даних та інші. Для оцінки рівнів доступності даних використовуються відомі системи, що визначають класи та категорії даних, які встановлюються за рекомендаціями експертів відповідної області, що представляє предметну область їх інтерпретації.

У роботі досліджується метод формального опису параметрів, що використовуються під час розв'язання задач з надання повноважень користувачам. Такі параметри характеризують інформаційні елементи, які описуються відповідними даними та параметрами інформаційних запитів прикладної задачі, для розв’язання якої потрібні відповідні дані. До параметрів, що характеризують елементи інформації, належать наступні: рівень конфіденційності відповідних даних, характер їх важливості та інші. Рівень конфіденційності різних даних, на початковому етапі, визначається за рекомендаціями експертів. Зміна рівнів конфіденційності в процесі функціонування системи може здійснюватися автоматично або шляхом надання рекомендацій відповідним експертом щодо здійснення відповідних змін. Параметр важливості даних визначається частотою їх використання.

Побудова методу визначення параметрів інформаційних компонентів та методу визначення параметрів інформаційних запитів задач ґрунтується на спільних принципах. Розроблено способи визначення відповідних параметрів на основі аналізу потреб предметної області, що обслуговується відповідною інформаційною системою, та на основі вимог із забезпечення, в кінцевому випадку, необхідного рівня безпеки інформаційної системи. На основі побудованих визначень розроблено способи обчислення значень їх величин, що дозволило враховувати відповідні параметри при реалізації процесів захисту, з різним рівнем їх ефективності.

Дворівнева модель надання повноважень на використання даних різних рівнів конфіденційності функціонує наступним чином. На першому рівні надання повноважень відповідна система аналізує повноваження користувача, який звертається до системи для отримання даних. Перевіряються ідентифікаційні дані користувача та дані, що визначають його право на доступ до даних певних рівнів конфіденційності. Користувач, який звертається до системи, крім власних даних, повинен надати системі відомості про задачу, для розв’язання якої потрібні відповідні дані. У випадку, коли дані, за якими звернувся користувач, відносяться до вищих рівнів конфіденційності і не повинні надаватися користувачу, то система надання повноважень переходить на другий рівень. На цьому рівні функції користувача виконує прикладна задача, що була представлена користувачем – фізичною особою, і в цьому випадку така задача називається користувачем – задачею. На цьому рівні система надання повноважень проводить аналіз параметрів інформаційних запитів задачі і на його основі приймає рішення про можливість надання даних задачі або ж приймає рішення щодо забезпечення умов, які гарантують можливість вирішення зазначеної задачі. Важливим аспектом функціонування системи надання повноважень на другому рівні є те, що користувач – фізична особа не має можливості впливати на прийняття системою рішення щодо надання повноважень на отримання даних задачею або сприяти забезпеченню можливості розв'язання цієї задачі. Це означає, що під час роботи з даними високого рівня конфіденційності у користувача відсутня можливість вплинути на розв'язання

задачі, виходячи з певних суб'єктивних факторів чи інших причин, які можуть мати відношення до нього.

На другому рівні надання доступу відповідна система може виконувати цілий ряд функцій із забезпечення процесу розв'язання прикладної задачі. Для реалізації таких функцій система надання повноважень аналізує дані про предметну область інтерпретації, яку вона обслуговує. Прикладом однієї з можливостей із забезпечення розв’язання прикладної задачі може слугувати наступна можливість системи. Для обраного рівня конфіденційності даних система містить алгоритми, якими можуть перетворюватися відповідні дані. Система надання повноважень обирає алгоритм перетворення даних, який найбільшою мірою відповідає фрагменту алгоритму, що реалізується в задачі і призначений для перетворень цих даних, за якими звертається задача, та за результатами чого здійснює відповідні перетворення даних. Завдяки цьому система не передає дані задачі, а передає їй результат перетворення відповідних даних, який має рівень конфіденційності нижчий, ніж рівень конфіденційності даних, які перетворювалися. Цей підхід ґрунтується на тому, що дані відповідного рівня конфіденційності можна перетворювати тільки обмеженою кількістю алгоритмів. Це обмеження встановлюється на основі аналізу інтерпретації відповідних даних у предметній області інтерпретації, яку обслуговує відповідна інформаційна система.

У роботі досліджується метод моделювання процесу функціонування дворівневої системи надання повноважень різним типам користувачів. Оскільки процеси функціонування системи надання повноважень тісно пов'язані з предметною областю інформаційної системи, то в роботі запропоновано ряд характеристик та особливостей предметної області інформаційної системи. Прикладом таких характеристик можуть бути уявлення про критичні події, що можуть виникати у середовищі, на обслуговування якого орієнтована система. Доводиться твердження про те, що використання результату розв'язання задачі в предметній області не призведе до виникнення в ній суперечностей, якщо мета задачі не суперечить умовам, що характеризують предметну область, яку обслуговує інформаційна система. У роботі вводяться визначення параметрів інформаційних

запитів задачі, які характеризують задачу, як таку, розв’язання якої доцільно розв'язувати та використовувати в предметній області. Прикладом такого параметру є параметр актуальності задачі, що визначається на основі аналізу середовища, яке обслуговує інформаційна система.

Крім параметрів моделей даних, якими є інформаційні елементи, та параметрів інформаційних запитів прикладної задачі, в роботі досліджуються інформаційні характеристики відповідних задач, що тісно пов'язані з предметною областю інтерпретації інформаційної системи. Такими інформаційними характеристиками є: розширення предметної області даними, що отримані в результаті розв'язання прикладної задачі, перевірка, чи поточна задача не є повторенням раніше вирішеної прикладної задачі, чи поточна задача використовує одні й ті ж вхідні дані, що і попередня задача, але має відмінну від попередньої задачі мету. Вводиться параметр обґрунтованості використання даних поточною задачею, який визначається величиною співпадання цілей задач, одна з яких використовує деякі вхідні дані, а друга їх не використовує. Очевидно, що коли цілі таких двох задач достатньо близькі, то значення параметру обґрунтованості використання відповідних даних задачею є малим.

Для реалізації процесу побудови багаторівневої моделі надання повноважень водиться ряд положень, які визначають умови використання відповідної системи. Прикладом такого положення є вимога, яка стосується необхідності інтерпретації даних, які використовуються прикладними задачами, які узгоджуються з інтерпретаціями компонентів, що входять до складу предметної області інтерпретації, та обслуговуються інформаційною системою. Доводяться твердження про обмеженість множини критичних ситуацій та аномалій, які можуть виникати в предметній області інтерпретації інформаційної системи. Доводяться також твердження про те, що система засобів, які використовуються системою надання повноважень на використання відповідних даних, є повною відносно задач. У роботі приймається, що необхідність тих чи інших рівнів конфіденційності даних визначається можливим рівнем втрат. До цих втрат може призвести використання результатів розв'язання, які отримані несанкціонованими прикладними задачами.

Використання цих результатів може відбуватися лише в предметній області інтерпретації інформаційної системи.

Важливим компонентом системи надання повноважень є система прийняття рішень, використання якої дозволяє співпрацювати з прикладною задачею, яка потребує даних, що мають найвищі рівні конфіденційності. Оскільки необхідний рівень конфіденційності даних визначається рівнем втрат, до яких може призвести використання результатів, отриманих несанкціонованими задачами у відповідній предметній області інтерпретації, що використовує відповідні дані, то можливість пониження рівня конфіденційності даних, при використанні результатів розв’язання санкціонованих задач, може призвести до підвищення рівня безпеки інформаційної системи, що безпосередньо пов'язана з безпекою процесів, які відбуваються в предметній області інтерпретації цієї інформаційної системи.

Для коректного використання інформації з предметної області інтерпретації інформаційної системи, необхідно ввести ряд критеріїв, що визначають різний характер змін у цій області. Такими критеріями, що використовуються системою надання повноважень, є критерії, які визначають прогресивність змін, що відбуваються в області інтерпретації, при впровадженні в неї результатів розв'язання прикладних задач. Прикладом таких критеріїв є критерії зниження рівня конфіденційності даних, які використовуються в предметній області інтерпретації за рахунок використання в цій області результатів розв'язання прикладних задач. Наступний приклад критерія прогресивності змін в предметній області інтерпретації інформаційної системи полягає у тому, що якщо в результаті розв'язання прикладної задачі в предметній області інтерпретації зникають аномалії або критичні ситуації, то така прикладна задача є актуальною, а зміни, які відбуваються у прикладній області при використанні результатів розв'язання такої задачі, є прогресивними. У роботі аналізуються відмінності між уявленнями про надійність системи та уявленнями про безпеку системи. Це дозволяє підкреслити важливість задач, пов'язаних із забезпеченням безпеки системи, яка незалежно від надійності відповідної системи, орієнтована на виконання власних функцій забезпечення її безпеки.

У роботі розроблено алгоритми розв'язання задач, що досліджувалися та були розв'язані. Ці алгоритми представлено відповідними блок-схемами. Одна з таких блок-схем демонструє процеси надання повноважень на використання даних, що мають певні рівні конфіденційності, а друга блок-схема описує алгоритм загальної організації процесу функціонування системи надання повноважень користувачам. Зазначені блок-схеми підтверджують можливість практичного використання розроблених у роботі методів надання повноважень користувачам на використання даних різних рівнів конфіденційності.

ПУБЛІКАЦІЇ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Суліма О.А. Аналіз впливу параметрів даних на процеси надання повноважень / О.А. Суліма // Моделювання та інформаційні технології: Зб. наук. праць ІПМЕ НАН України. – Київ, 2016 – с. 110-118.

2. Суліма О.А. Розробка алгоритму надання повноважень задачам на використання даних / О.А. Суліма // Моделювання та інформаційні технології: Зб. наук. праць ІПМЕ НАН України. – Київ, 2016 – с. 110-116.

3. Давиденко А.М. Використання формальних засобів опису процесів надання повноважень / А.М. Давиденко, О.А. Суліма // Захист інформації – Київ, 2016. - Том 18. - №2. - С.143-149

4. Суліма О.А. Аналіз основних систем надання повноважень користувачам. / О.А. Суліма // Моделювання та інформаційні технології: Зб. наук. праць ІПМЕ НАН України. – Київ, 2017 – с. 66-74.

5. Суліма О.А. Аналіз методів оцінок рівня безпеки доступу до даних. / О.А. Суліма // Моделювання та інформаційні технології: Зб. наук. праць ІПМЕ НАН України. – Київ, 2017 – с. 35-42.

6. Суліма О.А. Модель багаторівневої системи доступу / О.А. Суліма // Безпека інформації – Київ, 2017. –Том 23. – с. 123-130.

7. Сулима О.А. Основные тенденции развития киберпреступности на рубеже 2015 года. /О.А. Сулима // Моделювання: XXXIV науково-технічна конференція. – Київ, К.: ІПМЕ ім. Г.Е.Пухова НАНУ, 2015. – с. 27.

8. Суліма О.А. Особливості використання засобів визначення повноважень в державних інформаційних системах / О.А. Суліма // Моделювання: XXXV науково-технічна конференція. – Київ, К.: ІПМЕ ім. Г.Е.Пухова НАНУ, 2016. – 30 с.

9. Суліма О.А. Аналіз процесів надання повноважень в інформаційно-телекомунікаційних системах / О.А. Суліма // Фундаментальні та прикладні дослідження у сучасній науці: IV наукова конференція. – Харків, Х.: Технологічний центр, 2016. – С. 67-68.

10. Суліма О.А. Побудова моделі доступу на базі моделі Діона. / О.А. Суліма // Міжнародна наукова конференція "Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення (випуск 21)" / Збірник тез доповідей: випуск 21 (м. Тернопіль, 12 липня 2017 р.). – Тернопіль. – 2017. – с. 55-57.

11. Суліма О.А. Визначення оцінок параметрів в системі надання повноважень / О.А. Суліма // Наукова конференція "Наука та інформація" . – Київ. Альманах– 2017. – с. 84-91.

ABSTRACT

Sulima O. Methods of access security organizing to information systems based on multilevel models. – Manuscript.

A Thesis for the Academic Degree of Candidate of Technical Sciences. Specialty 05.13.21 Information security systems. – National Aviation University. Kyiv, 2017.

The thesis by Sulima O. focuses on the importance of solving tasks to increase the level of protection of information systems from unauthorized access to their data.

The purpose of the study is to solve the scientific and applied task of constructing information security means in information systems based on the use of a multilevel system of empowerment of users. To achieve the goal, the challenger has solved the following tasks: methods of assessing the level of authority for the use of data of different levels of their confidentiality are developed; the basic elements for the practical introduction of a two-tier system of empowerment for user data usage have been developed; methods of estimating the parameters of information elements and parameters of the information request of applied problems for the solution of which data are necessary in the information

system are developed; the components of a two-tier system have been developed to empower users to use data.

The scientific novelty of the obtained results is as follows: for the first time a method for determining the parameters of information requests for applied tasks has been developed, which allowed to broaden the analysis of the conditions that determine the possibility of empowering the applied task of using data; a two-tier model has been developed for empowering users to use data that access them to the information system; the main components of the two-tier data access model were first developed; it is proposed to apply the distribution of access levels to data, depending on the degree of their confidentiality, which function independently of each other.

The personal contribution of the applicant is that the author himself has received the main results of work, which is confirmed by personal publications in scientific publications and practical applications.

The structure of the dissertation consists of the introduction, four sections, conclusions, list of sources used and applications. The work is outlined on 193 pages and contains 164 pages of the main text.

The first chapter analyzes well-known methods for empowering users to use the data they access to the information system. The most common model for granting authority is the matrix model for access to data. This model provides for the possibility of granting different types of data usage permissions. An example of such authority is: the authority to read data; data write authority and others. Known systems that define the classes and categories of data, which are determined by the recommendations of the experts of the relevant area, representing the subject area of their interpretation, are used to assess the data availability levels.

The paper examines the method of the formal description of the parameters used in solving tasks of empowering users. Such parameters characterize the information elements that are described by the relevant data and parameters of the application's information requests, for which the relevant data is required. The parameters that characterize the elements of information include the following: the level of confidentiality of the relevant data, the nature of their importance, and others. The level of confidentiality of various

data, at an early stage, is determined by expert advice. The change in the level of confidentiality in the operation of the system can be done automatically or by providing advice by the relevant expert on making the appropriate changes. The parameter value of data is determined by the frequency of their use.

The construction of the method for determining the parameters of information components and the method for determining the parameters of information requests of problems is based on common principles. The methods of determining the appropriate parameters on the basis of analysis of the needs of the subject area serviced by the relevant information system and on the basis of requirements for ensuring, eventually, the necessary level of security of the information system are developed. Based on the constructed definitions, methods for calculating its value have been developed, which allowed taking into account the corresponding parameters in the implementation of the protection processes, with different levels of their effectiveness.

The two-level model for empowering the use of data of different levels of confidentiality functions as follows. At the first level of empowerment, the system examines the authority of the user who accesses the system for obtaining data. The user's identification data and data that determine his right to access data at certain levels of confidentiality are checked. User, which accesses the system, in addition to its own data, must provide the system with information about the task that requires appropriate data to be resolved. In the case where the data requested by the user are related to higher levels of privacy and should not be provided to the user, the system of privilege passes to the second level. At this level, the user function performs an application task that was presented by the user – an individual, and in this case, such a task is called the user – a task. The system of empowerment analyzes the parameters of the task information requests and, on the basis of it, makes a decision on the possibility of providing the data of the task or decides to provide conditions that guarantee the possibility of solving the specified task. An important aspect of the functioning of the system of empowerment at the second level is that the individual – the individual is not able to influence the decision–making system by the authority to grant the data to the task or to facilitate the possibility of solving this task. This means that while working with high–level privacy data, the user

is not able to influence the solution of a task, based on certain subjective factors or other reasons that may be relevant to it. At the second level of access, the appropriate system can perform a number of functions to provide a process for solving the application problem. To implement such functions, the system of empowerment analyzes data on the subject area of interpretation that it serves. An example of one of the possibilities for solving an application problem can be the following system capability.

For the selected data privacy level, the system contains algorithms that can be converted to the corresponding data. The system of granting powers selects an algorithm for data transformation, which most closely corresponds to the fragment of the algorithm that is implemented in the task and is intended for the transformation of these data, which the task is addressed, and the results of which carry out appropriate data transformations. Due to this, the system does not transmit the task data, but passes it the result of the conversion of the relevant data, which has a lower level of confidentiality than the level of confidentiality of the transformed data. This approach is based on the fact that data of the appropriate level of confidentiality can be transformed only by a limited number of algorithms. This restriction is established on the basis of an analysis of the interpretation of the relevant data in the subject area of interpretation served by the relevant information system.

The paper examines the method of modeling the functioning of a two-tier system of empowerment for different types of users. Since the processes of functioning of the system of empowerment are closely related to the subject area of the information system, a number of characteristics and features of the subject area of the information system are proposed in the paper. An example of such characteristics may be the idea of critical events that may occur in the environment for which the system is oriented. There is a statement that the use of the result of the problem in the subject area will not lead to contradictions in it if the purpose of the task does not contradict the conditions, which characterize the subject area served by the information system. In this paper, the definition of the parameters of the information requests of the task is introduced, which characterize the task as such, the solution of which it is expedient to solve and use in the subject area.

An example of such a parameter is the relevance of a task, which is determined on the basis of the analysis of the medium served by the information system.

In addition to the parameters of the data models, which are the informational elements, and the parameters of the information requests of the application, in the study the information characteristics of the corresponding problems, which are closely related to the subject domain interpretation of the information system. Such information characteristics are: expansion of the subject area data obtained as a result of the decision of the application, verification, whether the current task is not a repetition of a previously solved application task, does the current task use the same input data as the previous task, but differs from the previous objective goal. The parameter of the validity of data usage by the current task is introduced, which is determined by the magnitude of matching the objectives of the tasks, one of which uses some input data, and the second does not use them. Obviously, when the goals of such two problems are sufficiently close, the value of the parameter of validity of the use of the corresponding data by the problem is small.

To implement the process of constructing a multi-level model of empowerment there is a number of provisions that determine the conditions of use of the system. An example of such a provision is the requirement that the interpretation of the data used by the application tasks is necessary, which are consistent with the interpretations of the components that are part of the subject area of interpretation, and are served by the information system. There is an assertion about the limited number of critical situations and anomalies that may arise in the subject area of the interpretation of the information system. It is also argued that the system of means used by the system for granting authority to use the relevant data is complete in relation to the tasks. The paper assumes that the need for certain levels of confidentiality of data is determined by the possible level of losses. These losses can be caused by the use of solution results obtained by unauthorized applications. The use of these results can occur only in the subject area of interpretation of the information system.

An important component of the empowerment system is the decision-making system, the use of which allows collaboration with an application task that requires data with the highest levels of confidentiality. Since the necessary level of data confidentiality is

determined by the level of losses that could result from the use of results obtained by unauthorized tasks in the relevant subject area of interpretation using the relevant data, the possibility of lowering the level of confidentiality of data, using the results of solving authorized tasks, may lead to an increase the level of security of the information system, which is directly related to the security of processes occurring in the subject area of interpretation of this other information system.

For the correct use of information on the subject area of interpretation of the information system, it is necessary to introduce a number of criteria defining the different nature of changes in this area. Such criteria used by the system of empowerment are criteria that determine the progressiveness of the changes taking place in the field of interpretation, when implementing the results of its application. An example of such criteria is the criteria for reducing the level of confidentiality of data used in the subject area of interpretation due to the use in this area of the results of the solution of applied problems.The following example of the criterion of the progressiveness of the changes in the subject area of the interpretation of the information system is that if as a result of the solution of an applied problem in the subject area of interpretation abnormalities or critical situations disappear, then such an application problem is relevant, which occur in the applied area when using the results of solving such a problem, are progressive. The paper analyzes the differences between representations about the reliability of the system and representations about the security of the system. This allows emphasizing the importance of tasks related to the security of the system, which, regardless of the reliability of the system, is oriented to fulfill its own functions to ensure its security.

In the work, algorithms for solving problems that were investigated and solved were developed. These algorithms are represented by the corresponding block diagrams. One of these flowcharts demonstrates the processes for empowering the use of data having certain levels of confidentiality, and the second block diagram describes the algorithm of the overall organization of the process of operating the system of empowering users. The indicated flowcharts confirm the possibility of practical use of the methods developed in the work of empowering users to use data of different levels of confidentiality.

Keywords: confidentiality, powers, access, data, applied task parameters, information system.

ВСТУП

Актуальність. Проблеми захисту та оцінки даних інформаційних систем на даний час продовжують залишатися надзвичайно актуальними. Особливо важливими є завдання, пов’язані з оцінкою та захистом даних у системах, орієнтованих на співпрацю з обраними об’єктами та відповідними середовищами. Головна мета захисту інформаційних даних полягає у тому, щоб виключити можливість їх несанкціонованого використання або втрат у відповідному середовищі. Важливим напрямом протидії таким ситуаціям є метод, який полягає у захисті даних шляхом надання останніх тільки тим користувачам, які мають відповідний допуск. Такий метод ґрунтується на реалізації різних способів оцінки даних, на основі яких приймаються рішення про їх надання чи не надання конкретному користувачу. Очевидно, що в рамках реалізації цього методу необхідно і важливо контролювати користувача, який має право на використання тих чи інших даних з відповідних інформаційних систем. Розпізнавання користувачів полягає у визначенні допуску конкретного користувача та його повноважень на отримання і використання відповідних даних. Зазначені аспекти приведеної проблеми розв’язують системи доступу до даних, за якими звертаються користувачі.

Іншою складовою цієї проблеми є оцінка даних, яка визначає необхідний рівень їх захисту та може умовно називатися рівнем конфіденційності. Рівень конфіденційності є основним чинником для прийняття інформаційною системою рішення про надання чи не надання відповідних даних користувачу, який звернувся за їх отриманням.

На сучасному етапі розвитку інформаційних систем оцінка рівня конфіденційності, на відміну від минулих уявлень, не є сталою, навіть у випадку, коли одночасно з декларацією рівня конфіденційності декларується період, протягом якого відповідна оцінка повинна зберігатися. Ці оцінки змінюються з часом під впливом різних факторів, що характеризують середовище, до якого відносяться відповідні дані. Такі зміни можуть призводити до зміни рівня повноважень користувачів.

Наведені аспекти ілюструють складність задач, пов’язаних з оцінкою даних і, відповідно, з рівнем їх захисту та реалізуються через управління доступу до них користувачів, які мають різні права на використання таких даних. У зв’язку з цим задачі, що досліджуються та розв’язуються у дисертаційній роботі, є важливими та актуальними для подальшого практичного впровадження.

Аналогічними проблемами займається ряд відомих вчених, зокрема: Д. Белл, Л. Лападула, А. Йонез, Р. Ліптон, І. Снайдер, Л. Діон, Р. Сандху, Е. Койн, А. Файнстайн, К. Йомен, К. Ландвер, К. Хайтмайер, Дж. Маклін, Д. Кларк, Д. Уілсон, Дж. Міллен, К. Біба, М. Харрісон та інші.

Беручи до уваги наведене вище, є підстави вважати, що тема дисертаційної роботи є новою та актуальною.

Зв'язок роботи з науковими програмами, планами, темами. Робота виконувалася у рамках замовлень наукових досліджень Президії Національної академії наук України в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова (ІПМЕ): «Дослідження та розробка методів оцінювання захищеності інформації в розподілених високопродуктивних інформаційних системах при вирішенні задач енергетики» (шифр МОД-Д, реєстраційний номер 0114U002361, 2014-2017 рр.).

Мета і задачі дослідження. Мета роботи полягає у вирішенні науково-прикладної задачі, спрямованої на побудову інформаційних засобів для реалізації методів підвищення рівня захисту даних в інформаційних системах на засадах використання багаторівневої системи надання повноважень та застосування автоматизованого процесу визначення поточних значень рівня конфіденційності даних. Зазначене дозволяє забезпечити необхідну зміну рівня їх конфіденційності в процесі функціонування інформаційних систем. Для досягнення поставленої мети **необхідно було розв’язати наступні задачі:**

– здійснити аналіз існуючих методів надання повноважень користувачам на використання даних з інформаційних систем, за підсумками чого визначити необхідність подальших досліджень, пов’язаних з методами надання повноважень на використання даних різних рівнів конфіденційності;

– розробити метод формального опису параметрів, що характеризують моделі даних інформаційної системи;

– розробити метод оцінки параметрів інформаційних запитів задач, що представляють собою дані, які знаходяться в системі захисту, що функціонує в рамках інформаційної системи;

– визначити компоненти моделі багаторівневої системи доступу;

– розробити метод визначення параметрів додаткових компонентів системи доступу, що дозволить керувати процесом доступу до інформаційної системи;

– розробити алгоритм реалізації основних процесів, що функціонують в системі доступу до інформаційної системи;

– розробити алгоритм загальної організації роботи дворівневої системи доступу до даних.

Об’єктом досліджень є організація процесу доступу до інформаційних ресурсів.

Предметом досліджень є методи доступу до інформаційних ресурсів.

Методи дослідження. Для розв’язання задач побудови багаторівневих моделей, формування рішень про надання повноважень використовувалися методи математичної логіки і семантичного аналізу, комп’ютерне моделювання та теорія інформаційних систем.

Наукова новизна отриманих результатів. У дисертаційній роботі розв’язана та досліджена нова науково-прикладна задача, що полягає у розробці та дослідженні методів захисту даних у спеціалізованих інформаційних системах від несанкціонованого доступу на основі використання багаторівневої моделі доступу та методу оцінки рівня їх захисту.

Наукова новизна отриманих результатів полягає в наступному:

– *удосконалено* метод формального опису параметрів інформаційних моделей даних, які за рахунок обчислення таких величин дозволяють більш повно їх оцінювати, співставляючи з необхідними рівнями захисту;

– *вперше розроблено* метод визначення параметрів інформаційних запитів задач та їх оцінок, який на основі використання характеристик конфіденційних даних з

інформаційної системи, незалежно від користувача, що представив відповідну задачу, дозволить приймати рішення системою про надання повноважень передачі задачі відповідних даних, при цьому стає можливим уникнути небезпек у результаті впливу суб'єктивних факторів користувача;

– *вперше розроблено* метод визначення параметрів додаткових компонентів засобів доступу до інформаційної системи, який за рахунок аналізу предметної області, що обслуговується інформаційною системою, дозволяє співставити рівень конфіденційності даних з величинами параметрів, які зазначені в інформаційному запиті задачі, яка звернулася із запитом, що дає змогу встановити залежність між рівнем захисту системи та умовами предметної області з використання результатів розв'язання прикладних задач;

– *вперше розроблено* основні компоненти дворівневої моделі доступу до даних, у якій відповідні рівні функціонують незалежно, але при переході з нижчого рівня на вищий також враховується результати перевірок нижчого рівня, за рахунок чого з'являється можливість уникнути впливу нижчого рівня на вищий при розв'язанні задач доступу до інформаційного ресурсу, що дозволяє надання інформації з високим рівнем конфіденційності узалежнити від цілі розв'язання задачі та узалежнити від характеру впливу використання цього розв'язання в предметній області, яку обслуговує інформаційна система.

Практичне значення результатів та їх впровадження. Отримані в дисертаційній роботі результати використовувалися для створення алгоритмів та реалізації програмних засобів, розв'язання задач захисту конфіденційних даних з різним рівнем конфіденційності, які забезпечують необхідний рівень захисту в процесі функціонування інформаційної системи.

Практична цінність роботи полягає в наступному:

– на основі запропонованої дворівневої моделі захисту даних розроблено алгоритм, який реалізує процес надання повноважень задачам, що звертаються за конфіденційними даними та розроблено відповідну блок-схему;

– на основі запропонованих елементів засобів доступу до інформаційної системи розроблено алгоритм загальної організації роботи дворівневої системи доступу до

даних, що забезпечує елімінацію суб'єктивних факторів користувача, які могли б впливати на можливість доступу до конфіденційних даних.

Розроблені методи організації доступу до даних використовувалися в Інституті кібернетики ім. В. М. Глушкова НАН України при проведенні первинної державної експертизи, що дозволило використовувати системи оцінювання ризиків безпеки інформаційних ресурсів в умовах великих обсягів консолідованої інформації та підвищити ефективність і рівень автоматизації процесів управління ризиками при побудові комплексних систем захисту інформації та систем менеджменту інформаційної безпеки».

Результати дисертаційної роботи впроваджено до навчального процесу НАУ і використовуються на кафедрі БІТ під час викладання дисципліни «Управління інформаційною безпекою».

Особистий внесок здобувача. Основні положення і результати дисертаційної роботи, що виноситься до захисту, отримано автором самостійно. У роботі [74], опублікованій у співавторстві, автору належить аналіз методів та засобів опису процесів надання повноважень.

Апробація результатів дисертаційної роботи. Основні наукові результати та положення дисертаційної роботи доповідалися на міжнародних і національних науково-технічних конференціях та семінарах, зокрема: «Моделювання: XXXIV» науково-технічна конференція (Київ 2015 р.); «Фундаментальні та прикладні дослідження у сучасній науці» IV наукова конференція (Харків 2016 р.); «Моделювання: XXXV» науково-технічна конференція (Київ 2016 р.); «Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення» міжнародна наукова конференція (Тернопіль 2017 р.).

Публікації. Основний зміст дисертаційної роботи викладено в 11 наукових працях, серед яких шість статей надруковано у фахових виданнях України; дві увійшли до наукометричної бази даних Index Copernicus [3, 6], п'ять тез та матеріалів у збірниках наукових конференцій.

Структура та обсяг дисертації. Дисертаційна робота складається з вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. Роботу

викладено на 193 сторінках, які містять 164 сторінки основного тексту, дві таблиці, 11 рисунків, перелік використаних джерел з 132 найменувань та три додатки.

РОЗДІЛ 1 Задачі надання повноважень користувачам інформаційних систем

1.1 Аналіз основних систем надання повноважень користувачам

Сучасні інформаційні системи (*IS*), які орієнтовані на розв'язання різних задач, і відповідають функціональній орієнтації установ, що їх використовують та наповнюють відповідними даними, в основному орієнтовані на накопичення та збереження інформації з метою подальшого надання відповідних даних, у першу чергу, користувачам, які є працівниками цієї установи. Дані, що зберігаються в *IS*, характеризуються різними параметрами, один з яких представляє собою параметр важливості цих даних відносно деяких встановлених критеріїв або параметр рівня конфіденційності цих даних. У визначенні цей параметр приводить до наступних особливостей, що характеризують дані в *IS*:

– чим вищий рівень конфіденційності даних або чим більший рівень їх значимості, тим меншій кількості користувачів вони можуть надаватися;

– рівень конфіденційності даних з часом, який визначається інтервалом їх зберігання та використання, зменшується незалежно від статусу критерію, відносно якого був початково встановлений той чи інший рівень конфіденційності;

– типи задач, що повинні розв'язуватися в рамках установи, яка є власником *IS*, тісно пов'язані з рівнем конфіденційності даних, які ця задача потребує;

– кількість задач різних типів прямопропорційно пов'язана з рівнем конфіденційності даних, які вони використовують;

– в процесі розв'язання задач окремою установою в *IS* може виникати необхідність змінювати рівень конфіденційності даних в бік зменшення цього рівня або в бік його збільшення.

Наступним параметром, який характеризує дані, є параметр рівня зв'язності окремих даних між собою. Використання цього параметра приводить до наступних особливостей їх використання:

– лише між даними, що зберігаються в IS, існують взаємозв’язки, які визначають елементи структури середовища IS;

– в середовищі даних IS існують структури різних типів, що накладаються одна на одну, а тип структури визначається певною умовою використання тієї чи іншої структури відповідних даних;

– дані характеризуються параметрами, що визначаються різними типами інтерпретацій цих даних, які формуються на основі розв’язання задач, що використовують відповідні дані.

Важливим параметром, що характеризує дані в IS, є параметр, пов'язаний з часом існування та функціонування окремих даних і IS в цілому. Цей параметр приводить до виникнення наступних особливостей, що характеризують окремі дані інформаційної системи:

– уявлення про стабільність даних у часі;

– уявлення про динамічність даних, яке може характеризувати частоту їх використання, для розв’язання різних задач;

– залежності між часовими інтервалами стабільності параметрів в часі.

Приведені параметри та особливості, до яких призводять відповідні параметри, обумовлюють необхідність у використанні досить складних механізмів надання повноважень користувачам на використання тих чи інших даних. Такі повноваження характеризуються особливостями, які, певною мірою, обумовлюють можливість класифікації відповідних систем надання повноважень та визначають критерії або умови надання чи не надання відповідних повноважень.

Насамперед відзначимо, що системи надання повноважень в IS, можуть розділятися на наступні класи:

– системи надання повноважень на основі аналізу параметрів чи характеристик користувача, який звертається за отриманням тих чи інших повноважень (SPK);

– системи надання повноважень, що ґрунтуються на аналізі параметрів даних щодо яких користувач звертається до системи (SPZ);

– система надання повноважень, яка використовує різні аспекти приведених вище систем повноважень.

Перш ніж більш детально аналізувати системи наданих повноважень, розглянемо найбільш поширені типи систем надання повноважень, які будемо пов'язувати з приведеними вище класифікаціями та параметрами, що характеризують SWP.

У рамках відповідних підходів функції надання повноважень та функцій захисту доступу до даних в багатьох випадках розглядаються як єдине ціле [1, 2]. Оскільки бази даних переважно орієнтовані на збереження, накопичення та надання даних, то система доступу до даних розглядається як система безпеки відповідної бази даних [3, 4]. Тому в літературі досить часто, відповідні системи розглядаються, як системи безпеки.

Найбільш поширеною моделлю доступу є матрична модель доступу, в якій у першому стовпці матриці розміщаються користувачі, яких прийнято називати суб'єктами, а в першому рядку матриці розміщаються ідентифікатори даних чи їх груп, які називаються об'єктами. На перетині рядків, кожен з яких відповідає окремому суб'єкту та стовпців, кожний з яких відповідає певному об'єкту, розміщуються ідентифікатори повноважень відповідного суб'єкта по відношенню до відповідного об'єкта [5]. Загалом матрична модель записується у вигляді наступного співвідношення:

$$M = A(h_i, O_j, P_{ij}),$$

де A – матриця, h_i – суб'єкт з і-того рядка, O_j – об'єкт j – того стовпця, P_{ij} – повноваження суб'єкта h_i по відношенню до об'єкта O_j. Прикладом такого повноваження може служити читання даних, запис даних, модифікація даних, зміна повноважень та інші. Якщо $P_{ij} = 0$, то h_i не має повноважень до будь яких дій з O_j.

Очевидно, що матриця $A(h_i, O_j, P_{ij})$ в процесі функціонування IS може змінюватися, що витікає з приведених описів параметрів, що характеризують дані, які розміщаються в IS. Це призводить до того, що модель $M = A(h_i, O_j, P_{ij})$ може мінятися. Насамперед розглядаються зміни, що стосуються повноважень h_i по

відношенню до O_j. Це означає, що в процесі функціонування IS можуть змінитися повноваження користувача h_i, що є досить природним. В процесі функціонування IS можуть змінюватися об'єкти або суб'єкти. Такі зміни описуються додаванням або відніманням окремих рядків та стовпчиків відповідно. Для зміни повноважень в рамках існуючих множин $\{h_i\}$ та $\{O_j\}$, процеси цих змін вимагають введення сукупності правил, які можна було б активізувати у процесі функціонування IS. Така система правил була виведена в роботі, яка називається системою «прийми-перекажи». У цій системі використовуються суб'єкти, об'єкти та повноваження. Ця система правил описує наступні операції:

– операцію «перекажи»;
– операцію «прийми»;
– операцію «створи»;
– операцію «усунь».

Формально такі операції описують співвідношенням:

$[(x(\sigma) \to z)\&(x(g) \to y)] \to [y(h) \to z]$.

Це означає, що суб'єкт x переказує уповноваження h до об'єкту z або субєктові y за умови, що x має повноваження по відношенню до y.

Операція «прийми» описується співвідношенням:

$$[(y(\sigma) \to z)\&(x(t) \to y)] \to [x(h) \to z]$$

Це означає, що суб'єкт x приймає уповноваження h до об'єкту z за умови, що x має уповноваження t приймання повноважень.

Операція «утвори» формально описується співвідношенням:

$$(x\&\rho) \to (x(\rho) \to y)$$

Це означає, що коли x має повноваження ρ, то x може утворити зв'язок $x(\rho)$ з суб'єктом або об'єктом y.

Операція «усунь» формально описується співвідношенням:

$$[x(\rho) \to y] \to [x(\rho \backslash \sigma) \to y]$$

Якщо x має множину повноважень ρ по відношенню до y, то операція «усунь» дозволяє від повноважень ρ відняти повноваження σ і тоді x буде мати по відношенню до y повноваження $(\rho \backslash \sigma)$.

Очевидно, що використання цієї системи правил дозволяє модифікувати матричну модель $M = A(h_i, Oj, P_{ij})$ довільним чином. Така модифікація визначається додатковими умовами, що можуть виникати в процесі функціонування бази даних [6].

Інший тип моделі доступу ґрунтується на використанні оцінок даних, до яких користувачі подають запит на використання. Очевидно, що для реалізації цього підходу повинна існувати певна оцінка потенціальних користувачів [7]. Тоді надання чи не надання доступу ґрунтується на співставленні такої оцінки. Прикладом такого типу моделі є модель Белла-Лападули [8,9].

У цій моделі кожний об'єкт має рівень захисту. Кожний рівень захисту описується класами і множиною категорій [10]. Класифікація представляє собою множину класів, що представляє собою наступне:

– явні (J);
– з обмеженим доступом або «для службового використання» (P);
– таємні (T);
– надзвичайно таємні (S).

Множина класу $K = \{J \prec P \prec T \prec S\}$ є упорядкована. Множина категорій встановлюється на основі аналізу середовища, в якому відповідні дані можуть використовуватися [11,12]. На основі аналізу середовища визначають множину категорій, які характеризують відповідні класи даних. Таким чином, у даному підході не класифікуються безпосередньо користувачі, а останні відносяться до згаданих категорій, які характеризуються як певні елементи середовища. Прикладом можуть служити такі категорії як військовий штаб армії, штаб полку, і т.д. [13]. У цьому випадку рівень безпеки буде позначатися L_i і можна записати, що $L_i = (K_i, C_i)$ є вищий або рівний рівню безпеки $L_j = (K_j, C_j)$, якщо виконуються співвідношення

$K_1 \succ K_2, C_1 \supseteq C_2$, що формально можна записати у вигляді наступного співвідношення: $\left[\left(K_i \geq K_j\right)\&\left(C_i \supseteq C_j\right)\right] \rightarrow \left(L_i \geq L_j\right)$.

Досить важливими поняттями, які використовуються при побудові моделей безпеки, є поняття про стан безпеки системи. Для можливості формально описувати відповідне поняття, вводять наступне позначення:

– O – множина об'єктів;

– P – множина суб'єктів;

– L – множина рівнів безпеки.

Стан системи описується співвідношенням: $Q = (D, A, F_b, H)$, де D – множина активних повноважень суб'єктів до об'єктів, A – матриця повноважень, F_b – функція рівня безпеки, H – поточна ієрархія об'єктів. Множина D складається з трійок (ρ, o, t), де ρ – суб'єкт o – об'єкт, t – повноваження. Тоді $(\rho, o, t) \in D$. Функція рівня F_b описує перетворення: $F_b: O \cup P \rightarrow L$ [14]. У теорії захисту інформації використовуються також наступні аксіоми безпеки інформаційної системи:

– аксіома простої безпеки;

– аксіома признаної безпеки;

– аксіома сталості;

– аксіома зірки;

– аксіома недоступності об'єкту, не активного;

– аксіома незалежності початкового стану.

Розглянемо для прикладу, деякі з цих аксіом. Аксіома простої безпеки формується наступним чином. Суб'єкт може мати повноваження R до об'єкту тільки тоді, коли рівень авторизації суб'єкту є рівнем безпеки, який є вищим або рівним рівню безпеки об'єкту. Стан системи $Q = (D, A, F_b, H)$ виконує вимоги аксіоми простої безпеки тоді, коли для кожного елементу $A(\rho, o)$, який має повноваження R, виконується залежність $F_{ba}(\rho) \geq F_{bo}(o)$. Ця аксіома гарантує, що суб'єкт не буде мати повноважень доступу до інформації, яка знаходиться на більш високому рівні безпеки, ніж рівень безпеки авторизації суб'єкту.

Аксіома признаної безпеки означає, що для кожного суб'єкта ρ, кожного об'єкту o і кожного повноваження t виконується наступне співвідношення:

$$[(\rho, o, t) \in D] \rightarrow [t \in A(\rho, o)]$$

Це означає, що суб'єкт може використовувати тільки ті повноваження, які є авторизовані в матриці доступу A.

Аксіома зірки полягає в наступному. Стан безпеки $Q = (D, A, F_b, H)$ виконує аксіому зірки тоді, коли для кожного суб'єкта $\rho \in \rho^{/}$, при $\rho^{/} \subset P$, останній входить в множину суб'єктів, які не являються довіреними і, для кожного об'єкту $o_i \in O$ виконується співвідношення:

$$A\rho \in A(\rho, o) \rightarrow F_{bo}(o) \geq F_{bp}(\rho)$$

$$R \in A(\rho, o) \rightarrow F_{bo}(o) \leq F_{bp}(\rho)$$

$$W \in A(\rho, o) \rightarrow F_{bo}(o) = F_{bp}(\rho)$$

Ці співвідношення означають наступне. Суб'єкт, який не є довіреним (під відсутністю довіреності розуміється, що суб'єкт є авторизованим, але рівень безпеки авторизації є нижчий від рівня безпеки об'єкта) може мати повноваження $A\rho$ до об'єкту o, якщо рівень безпеки об'єкту G не нижчий ніж поточний рівень безпеки. Друге рівняння означає наступне. Суб'єкт, який не є довіреним, може мати повноваження R (повноваження на читання даних) до об'єкту, якщо поточний рівень безпеки суб'єкту є не нижчий, ніж рівень безпеки об'єкту. Третє рівняння означає наступне. Суб'єкт, який не є довіреним, може мати повноваження W (повноваження на запис даних) до об'єкту, якщо рівень безпеки об'єкту є рівнем поточному рівню безпеки суб'єкту [15].

Ці аксіоми описують ситуації, коли поточні рівні безпеки суб'єкту незалежних від рівня безпеки його авторизації знаходяться в рамках значень безпеки, що є відповідними поточним значенням рівня безпеки даних, з якими суб'єкт хоче працювати і цей факт описується в матриці доступу, то такий суб'єкт може здійснювати відповідні дії в системі. Ці аксіоми ілюструють той факт, що відповідна система є безпечна.

В процесі функціонування довільної інформаційної системи, здійснюються процедури запису, зчитування, переносу даних, з одного місця до іншого, витирання даних, їх модифікація та інші перетворення. У кожній системі існує структура, що відображає класифікацію даних, наприклад, по відношенню до рівня їх важливості. Тому важливою є задача відслідковування процесів, що відбуваються з даними, для того, щоб окремі компоненти даних, наприклад, «конфіденційних» не попадали до області пам'яті, у яких знаходяться данні, що відповідають рівню «для службового використання» і навпаки [16]. Крім цього, існує задача, яка полягає у забезпеченні інтегральності даних. Параметр безпеки означає, що данні в процесі функціонування системи не повинні модифікуватися [17]. У рамках процесу функціонування IS повинні аналізуватися процеси, що повязані з читанням та записом. Очевидно, що в даному випадку, мова йде про надання чи не надання тих чи інших повноважень.

Для розв'язання цих задач була розроблена модель Діона, яка представляє собою сукупність визначень та аксіом, що в рамках приведених визначень дозволяють відслідковувати можливості зміни рівнів безпеки даних в інформаційних системах [18].

До аксіом, які розроблені в рамках моделі Діона, можна віднести наступні аксіоми.

Аксіома міграції:

$[PBM(O_1) \geq PBM(O_2)]\&[PIM(O_1) \leq PIM(O_2)] \rightarrow (O_1 \rightarrow O_2)$.

Аксіома не порушення:

$[PNB(O_1) \geq PNB(O_2)]\&[PNI(O_1) \leq PNI(O_2)] \rightarrow (O_1 \rightarrow O_2)$.

Аксіома безпеки:

$[PBC(P) \geq BPB(O_1)]\&[\text{PBZ(P)} \leq BPB(O)] \rightarrow (O_1 \rightarrow O_2)$.

Аксіома інтегральності:

$[PIC(P) \leq BPI(O_1)]\&[PIZ(P) \geq BPI(O_2)] \rightarrow (O_2 \rightarrow O_1)$.

Аксіома не порушення при читанні:

$[BPB(P) \geq PNC(O_2)]\&[BPI(P) \leq PNI(O_2)] \rightarrow (P \rightarrow O_2)$.

Аксіома збереження рівня міграції при читанні:

$[BPB(P) \leq PBM(O_1)]\&[\text{BPI(P)} \geq PIM(O_1)] \rightarrow (O_1 \rightarrow P)$.

Позначення, що використовуються в приведених визначеннях, означають наступне:

BP – абсолютний рівень, B – безпека, PB – рівень безпеки, P – рівень, N – не порушення, M – міграція, I – інтегральність, Z – запис, C – читання. Таким чином, скорочення типу PIC означає рівень інтегральності при читанні, PBM означає рівень безпеки міграції і т.д.

Як коментар, до приведених аксіом можна сказати наступне: якщо аксіома міграції не була б виконана, то дані, що розміщені в об'єкті O_2, могли б бути перенесені до об'єктів, до яких вони не можуть бути переслані безпосередньо. Якби аксіома непорушення не виконувалась, то дані, пересилка яких до O_2 була б заборонена, могли б там опинитися при використанні в якості посередника об'єкту O_1. Аксіома інтегральності обумовлює для суб'єкта P, який хоче активізувати свою дію, необхідністю мати повноваження до читання даних з об'єкту O_1 і повноваження для запису цих даних в об'єкт O_2 і так далі.

Важливим методом розв'язання задач контролю доступу є метод, що ґрунтується на використанні уявлень про ролі. Поняття ролі ґрунтується на приписуванні можливостей доступу до об'єктів і в подальшому приписуванні відповідних ролей суб'єктам [19]. Використання ролей пов'язано з тим, що в багатьох організаціях повноваження користувача значною мірою визначаються його посадою, яку той чи інший користувач займає. У відповідності з прийнятими поняттями модель доступу, що ґрунтується на використанні уявлень про ролі, позначається скороченням $RBAC$ [20, 21].

Роль представляє собою суб'єкти, які є не відомими до того часу, поки відповідну роль не стане використовувати конкретна особа. Завдяки цій моделі є можливим встановлювати залежності між ролями та користувачами. Наприклад, дві різні ролі не можуть реалізовуватися однією особою.

Ролі можуть створювати ієрархічні структури, що призводить до того, що ролі вищого рівня ієрархії можуть управляти повноваженнями ролей, що знаходяться на нижчих рівнях ієрархії [22, 23].

У рамках моделі $RBAC$ реалізуються наступні повноваження:

– мінімальні повноваження представляють собою опис об’єктів та повноважень, які є необхідними для розв’язання відповідної задачі;

– розподіл обов’язків полягає в тому, що коли розв’язання задачі потребує співпраці двох користувачів, це призводить до створення двох незалежних ролей, необхідних для виконання відповідної задачі [24];

– абстракція даних полягає у реалізації прав доступу низького рівня (читання, запис і т.д.), які можуть бути об’єднанні в правах доступу високого рівня (передача рахунку чи його прийом) [25,26].

Формально така модель описується наступним чином:

– U – множина користувачів;

– P – множина повноважень;

– R – множина ролей;

– S – множина сесій;

– $u \in U$ – окрема ідентифікована особа;

– $r \in R$ – опис посади та обов’язків особи і її повноваження;

– $s \in S$ – приписи різних ролей вибраному користувачу.

Користувач може починати сесію встановлюючи свою приналежність до певної ролі. Один користувач може відкривати цілий ряд сесій [27,28]. Модель $RBAC$ виконує наступні операції:

– перевіряє повноваження користувача до певної ролі або приписує $PA \subseteq PR$ та приписує користувача до ролі або $UA \subseteq UR$ [29].

У рамках моделі реалізується наступна функція: користувачеві приписується одна сесія або $S \to U$ та кожній сесії приписується підмножина ролей або $S \to 2^R$. Це означає, що $rola(S) \subseteq \{(r/kopicnyba(S), r) \in UA\}$ [30].

У результаті сесія S має повноваження, яке описується наступним чином: $U_{r \in role(S)}\{P/(P,r) \in PA\}$.

На відміну від матричних моделей, у яких задаються користувачі h_i і об’єкти, яким приписуються повноваження $P(h_i, O_j)$, в моделі $RBAC$ визначаються ролі, до яких можна приписувати ті чи інші повноваження, а конкретні користувачі дістають

ті чи інші повноваження у випадку, коли вони займають ті або інші ролі, кожна з яких має певні повноваження. У рамках моделі $RBAC$ задається ієрархічна структура для ролей, яка, по суті, є відображенням ієрархічних структур взаємозалежностей між працівниками певної установи чи організації, яка встановлює відповідні повноваження для працівників [31].

Проблеми захисту баз даних досить широко досліджуються [32], що приводить до створення різних механізмів реалізації доступу до даних, що є досить близьким до уявлень про надання повноважень.

Виходячи з приведеного аналізу можна стверджувати, що надання повноважень та надання доступу представляють собою споріднені задачі.

У рамках даної роботи уявлення про надання доступу та надання повноважень розділяються наступним чином. Система захисту доступу і, відповідно, надання користувачеві доступу до системи, обов’язково проводить аналіз ідентифікаційних даних користувача і на основі цих даних надає чи не надає доступ до системи. Крім того система розв’язує задачу надання повноважень до реалізації в рамках бази даних певних функцій, які для баз даних є порівняно простими, наприклад, функції читання, запису, модифікації, перестановки, стирання даних, та інші [33].

Такий підхід призводить до того, що всі фактори, які обумовлюють безпеку системи, пов’язані з персональними даними користувача. Це в свою чергу, призводить до того, що для реалізації несанкціонованого втручання до бази даних, достатньо в певній мірі отримати доступ до ідентифікаційних даних користувача, які є персональними, і доступ до них може бути мало зв’язаний з самою базою даних [34]. Більше того, персональні дані, як правило, у тому чи іншому наближенні можуть використовуватися не тільки в рамках співпраці з окремою базою даних [35].

Існують досить широкі можливості несанкціонованого заволодіння частиною персональних даних чи всіма персональними даними. Несанкціонований доступ, у більшості випадків, є результатом проведення цільових досліджень відповідних систем доступу не уповноваженими користувачами. Для проведення таких

досліджень використовується неповна інформація про персональні дані уповноваженого користувача.

Таблиця 1

Результати аналізу основних систем та моделей надання повноважень

MC	*Q*	*W*	*E*	*R*	*T*	*Y*
Белла-Лападула	R	-	-	Z	-	-
Довірених суб'єктів	R	-	+	X	-	-
Розподілених систем	R	-	+	C	-	-
Адепт-50	R	-	-	C	-	-
LWM	R	-	+	Z	-	-
Лендвера	R	-	+	V	-	-
MAC	R	+	+	X	-	-
HRU	R	+	-	B	-	-
Кларка-Вілсона	R	-	-	Z	-	-
Міллена (MPP)	R	-	+	Z	-	-
MMS	R+	+	+	M	-	-
Біба	R-	-	-	N	-	-
Багаторівнева система доступу	R+	+	+	M	+	+

З метою проведення порівняльного аналізу існуючих основних систем та моделей надання повноважень та запропонованої у дисертаційній роботі багаторівневої системи доступу, уведемо наступні умовні позначення: MC – модель конфіденційності; HRU – модель Харрісона-Руззо-Ульмана; LWM – модель Low-Water-Mark; MZD – модель динамічної системи захисту доступу; MAC – модель мандатного доступу; Q – типи доступу, що використовуються в моделі; W – системний компонент; E – компонент безпеки; R – особливості операцій доступу суб'єкта до об'єктів; R– read, write; R+ – read, write, create, delete, операції з об'єктами специфічної структури; R- і Z – обмеження накладаються на найпростіші операції read, write; X – операції read, write можуть бути видаленими; C – забезпечує однорідний контроль права на доступ над неоднорідними множинами програм і даних, файлів, користувачів; V – частина цих обмежень повинна реалізовуватися користувачами системи, а частина системою; B – містить тільки одну умову; N – множини суб'єктів і об'єктів упорядковані відповідно до рівнів безпеки; M – крім найпростіших операцій у моделі можуть з'явитися операції, спрямовані на

специфічну обробку інформації; L – наявність ієрархії рівнів доступу, орієнтованих окремо на користувача і задачу; T – можливість отримання частки інформації з консолідованого блоку більш високого рівня конфіденційності; Y – дробове представлення способу доступу.

Зазначені данні зведемо у таблицю, яка наглядно демонструє переваги того чи іншого методу або моделі. Як видно з проведеного аналізу (табл. 1) запропонована багаторівнева система доступу має певні переваги перед іншими. Зокрема, вони полягають у наявності ієрархії рівнів доступу, орієнтованих окремо на користувача і задачу; можливості отримання частки інформації з консолідованого блоку більш високого рівня конфіденційності та дробове представлення способу доступу.

1.2 Аналіз методів оцінок рівня безпеки доступу до даних

Системи захисту доступу до баз даних чи до інформаційних систем завжди забезпечують певний рівень захисту, який є достатнім для окремої системи. У даному випадку не існує розподілу на системи захищені або не захищені. Це обумовлюється наступними факторами та особливостями:

– різні системи даних або інформаційні системи можуть містити дані, які мають різні рівні значимості або різні рівні їх важливості відносно заданого критерію такої значимості;

– засоби захисту доступу до системи, залежно від рівня захисту яку вони забезпечують, мають різну вартість, яка вимірюється, щонайменше, величиною обчислювальних ресурсів, які є необхідні для реалізації того чи іншого рівня захисту;

– захист, крім забезпечення санкціонованого доступу до даних, забезпечує можливість довготривалого зберігання відповідних даних, що в більшості випадків не приймається до уваги при дослідженні систем захисту доступу.

Будь-яка інформаційна система має певний рівень захисту навіть у тому випадку, коли при проектуванні системи не розглядалася задача формування окремих засобів захисту. Така ситуація має місце завдяки тому, що базові засоби, з

яких складається, наприклад, операційна система чи стандартна система, бази даних, мають засоби захисту, що закладаються при їх проектуванні незалежно від того, чи потенціальний користувач потребує чи не потребує захисту, відповідно поданої ним декларації про необхідні параметри системи [36]. Кожна система, як деякий продукт, повинна забезпечувати заданий рівень надійності [37]. У рамках цього параметру не виділяються причини, через які система перестала працювати. Серед можливих причин відмови системи важливе місце займає причина, що полягає у вразливості системи на зовнішні атаки. Виявлення і протидія таким атакам є безпосередньою задачею системи захисту, яка так чи інакше повинна бути реалізована в рамках довільної інформаційної системи.

Приведений аналіз ілюструє необхідність розв'язання наступних задач при проектуванні *IS*:

– визначення рівня безпеки функціонування системи або здійснення оцінки рівня безпеки системи;

– створення в рамках системи або у вигляді незалежної компоненти системи захисту;

– прогнозування зміни рівня безпеки системи з метою упередження можливої відмови системи;

– створення засобів управління рівнем захищеності системи в процесі її функціонування.

У даному випадку більш детально зупинимося на методиці оцінки величини безпеки системи [38]. У зв'язку з використанням уявлень про надійність системи та ряд інших понять і характеристик, зміна значень яких проявляється таким чином, які є подібним до прояву зниження рівня безпеки системи, необхідно мати можливість виявляти причини проявів тих чи інших відхилень. Тому приймемо, що рівень безпеки зменшується в результаті успішної дії зовнішніх атак на систему [39, 40]. Це означає, що система повинна в своєму складі мати засоби для виявлення таких атак. Завдяки таким засобам є можливим інтерпретувати зміну стану системи, як зниження поточного рівня безпеки системи. Оскільки прояв дії атак на систему не обов'язково полягає у відмові останньої, а може полягати у негативній зміні

параметрів функціонування системи, доцільно зниження рівня безпеки оцінювати в одиницях, які характеризували б вплив змін у системі на параметри, що характеризують зменшення показників якості функціонування [41].

Для випадку, коли об'єктом небезпеки є IS, приймаємо, що експерти, які працюють з системою, можуть встановити шкалу зміни рівня якості її функціонування, а фахівці з питань безпеки реалізують співставлення в рамках шкали якості, різним значенням якості різні рівні безпеки, якщо зниження рівня якості обумовлюються зовнішніми атаками.

Існуючі методи оцінки рівня безпеки орієнтовані на можливість їх використання для широкого класу інформаційних систем. Тому в таких підходах закладаються деякі загальні ознаки змін у процесі функціонування і на основі таких загальних ознак формуються моделі оцінки рівня безпеки [42].

Досить поширеним підходом до визначення оцінки рівня безпеки є підхід, у якому приймаються наступні тези. Перша теза полягає у тому, що зовнішня атака на IS виникає у випадкові моменти, а характер діючих атак змінюється залежно від успішності чи не успішності дії попередніх атак. Це означає, що на початку процесу функціонування IS рівень безпеки $RB(IS)$ приймає значення 100%.

У залежності від кількості успішних атак, RB може знижуватися. Якщо значення величини RB пов'язувати зі зниженням якості функціонування IS, то такі дані задають фахівці, що експлуатують IS. Відповідно до оцінки фахівців, встановлюються відповідні величини поточного рівня безпеки в процентах. Наприклад, зниження рівня безпеки на 30% призведе до того, що поточний рівень безпеки стає рівним 70%. Таким чином одна з моделей оцінки рівня безпеки може полягати у прогнозуванні кількості випадків успішних зовнішніх атак по відношенню до IS. У такому підході, умовно приймається, що кількість атак впливає на величенну зміни рівня безпеки. Досить поширеною оцінкою величини зміни рівня безпеки функціонування IS є величина ризику того, що система відмовить в обслуговуванні користувачам [43]. У залежності від інтерпретації всіх факторів, що входять до складу моделі, у даному випадку моделі ризику, який прийнято позначати R, стає можливим визначити деяку величину, що допускає інтерпретацію

зниження рівня безпеки R для системи IS. У рамках такого підходу зміна величини R залежить від параметрів потоку атак At_i, що подаються на IS. Для того, щоб зміну величини R можна було інтерпретувати відповідними змінами в IS, необхідно реалізувати моделювання дії різних атак на систему, що є досить громіздким та потребує значних затрат. Для вирішення цієї проблеми на рівні експертних оцінок встановлюються різні рівні зниження рівня безпеки у процентних величинах. Наприклад, може бути прийнято, що коли рівень безпеки RB знизився на 50%, то необхідно переходити до рівня моделювання дії атак на об'єкт, з метою активізації необхідних функцій протидії атакам.

Існують різні підходи до визначення величини ризику зміни рівня безпеки або для визначення поточного значення величини безпеки системи [44,45]. Один з таких підходів ґрунтується на експертних даних, які, практично, є деяким узагальненням статистичних даних про вплив різних параметрів на величину ризику, який відповідає тому чи іншому рівню безпеки. На відміну від ймовірнісних моделей, модель, що ґрунтується на експертних даних, є більш проста з точки зору її використання, а використання експертних даних виключає необхідність проводити додаткові дослідження для виявлення елементів, що входять до складу ймовірнісної моделі [46].

Підходом, який ґрунтується виключно на експертних даних є метод, що передбачає декларування областей значень всіх параметрів, що використовуються для визначення величини ризику. При цьому сама величина ризику також декларується по відношенню до встановлених діапазонів значень параметрів, що його визначають. Прикладом такого підходу може служити наступне [47].

Приймаються наступні параметри та їх значення:

– параметр вартості засобів, що оцінюються в масштабі умовно вибраних числових значень від 0 до 4;

– встановлено три рівні загроз, які визначаються як низький рівень загроз, середній рівень загроз та високий рівень загроз;

– визначена або прийнята шкала рівня піддатності засобів, яка визначається для кожного рівня загроз окремо шкалою, що складається з трьох діапазонів «низька

піддатність», «середня піддтаність» та «висока піддатність» засобів по відношенню до можливих атак або негативних зовнішніх впливів;

– кожній можливій позиції піддатності засобів для відповідного рівня загроз, окремо для кожного рівня ціни засобів захисту, приймається певна величина ризику, яка задається на множині цілих чисел.

При визначенні рівня загроз експертами приймаються до уваги наступні фактори.

Фактор 1. При здійсненні цільової атаки, яка реалізується несанкціонованою особою, аналізується наступне:

– оригінальність засобу, який наражається на атаку;

– легкість заміни отриманого засобу на очікувану вигоду від реалізації такого втручання;

– технічний рівень, що визначає можливість несанкціонованої особи успішно реалізувати своє втручання у роботу системи з метою отримання відповідного засобу або інформації.

Фактор 2. Можливість виникнення загрози (з точки зору ймовірності такої події).

Фактор 3. Вразливості або піддатності окремих засобів на несанкціоноване використання засобів системи та інші.

Перший і другий фактори є очевидними. Третій фактор полягає в наступному. Під вразливістю, у даному випадку, розуміється можливий рівень втрат від несанкціонованого втручання. Під піддатністю розуміється рівень складності реалізації послідовності дій зі сторони несанкціонованих факторів, які необхідно реалізувати для успішного здійснення атаки на систему. Якщо атака здійснюється з метою отримання даних з системи, то рівень піддатності відповідних компонентів системи може бути таким, що досить виявити ключ доступу до даних, щоб їх можна було несанкціоновано отримати. Це ілюструє рівень піддатності. Може мати місце ситуація коли для отримання можливості доступу до даних необхідно спочатку впровадити у систему «троянського коня», в якому можуть розміщатися інтрузи, які при виникненні певних умов у системі, можуть активізуватися і, наприклад, зчитати

відповідну інформацію і тільки після того несанкціонований користувач або атака зможе отримати відповідні дані.

Очевидно, що другий випадок ілюструє меншу піддатність системи на спроби несанкціонованого доступу до даних системи.

Величина ризику також задається у вибраному діапазоні чисел, наприклад, у діапазоні [0,8].

У рамках такого підходу для кожного засобу оцінюється зв'язана з ним піддатність та відповідна загроза. На основі приведених даних будується таблиця в першому рядку якої записується рівень загрози. У другому рядку таблиці записується рівень піддатності для кожного рівня загрози. Таким чином, якщо кількість рівнів піддатності є K, то, для кожного рівня загрози, вказуються всі K рівнів піддатності. Таким чином, у таблиці отримуємо $n = k \cdot m$ стовпців, де m-кількість рівнів загрози. У рядках цієї таблиці розміщаються рівні вартостей засобів, до яких може отримати доступ інтруз, під яким розуміється несанкціонований користувач чи атака. Наприклад, якщо вартість засобу є найвища, рівень загрози є найвищим, і рівень піддатності відповідних засобів є найвищим, то і величина ризику є найвища. Цей факт відображається шляхом запису відповідної величини ризику у клітині таблиці, яка знаходиться на перетині рядка і стовпця, що вибираються за приведеними вище ознаками. Це означає, що найвищий ризик може існувати лише при визначених умовах. Всі інші величини ризиків, що розміщаються в інших клітинах таблиці, визнаються на основі значень вартості інших засобів рівня загрози та рівня піддатності відповідний засобів.

Очевидно, що ці величини вибираються експертними методами. Слід відмітити, що найменша величина ризику, наприклад, рівна нулю, також може бути тільки в одній клітині відповідної таблиці.

Методи аналізу ризику повинні давати відповіді на цілий ряд питань, які безпосередньо пов'язані з безпекою інформаційної системи [48]. Прикладом таких питань може бути питання, які загрози є найбільш небезпечними для зниження рівня безпеки та значимість втрат від таких загроз [49]. Для відповіді на це питання досить просто сформувати відповідну таблицю, якщо користуватися експертними даними,

оскільки вони є найбільш повні, за визначенням, з точки зору інформації, яку вони можуть надавати. У цьому випадку можна побудувати таблицю, в кожному рядку якої описується небезпека, що буде складати перший стовпчик таблиці. У другому стовпчику таблиці описується вартість наслідків дії загрози, яка визначається експертним способом. У третьому стовпчику записується величина загрози або рівень загрози, який обумовлюється відповідною небезпекою. Ці величини також визначаються експертним способом. Тоді величину ризику відносно типу небезпеки можна визначати як результат множення величини втрат на величину загрози. Оскільки величина загрози є безрозмірна, то величина ризику буде вимірюватися в коштах, у яких вимірюється величина втрат від успішної дії окремої небезпеки. Відповідно до величини ризику можна встановити ранг різних небезпек з точки зору їх дії на систему.

При проектуванні інформаційних систем важливим є врахування всіх аспектів виникнення ризику по відношенню до окремої системи. Оскільки приймається, що будь-яка інформаційна система може піддаватися тим чи іншим атакам, доцільно встановити величину ризику, яка уже існує у середовищі незалежно від того чи певна інформаційна система уже реалізована, чи ні.

Це означає, що слід розділити ризики щонайменше на дві категорії: уже відомі можливі ризики, які обумовлюються атаками, що активізуються по відношенню до цих систем і з великою ймовірністю будуть активізуватися по відношенню до системи, що створюється, та ризики, які можуть виникнути в процесі функціонування окремої системи, що обумовлюються особливостями самої системи та характером даних, які передбачається розміщати в системі.

Необхідність у такому розподілі типів ризику обумовлюється тим, що будь-яка інформаційна система повинна мати певний рівень захисту від самого початку свого функціонування. Це обумовлюються тим, що будь яка інформаційна система, яка проектується, орієнтована на певний клас задач, розв’язання яких система повинна забезпечувати [50].

Результат розв’язання довільної задачі може представляти собою продукт, який має певну вартість. Коли системи використовуються для задач, що орієнтовані на

обслуговування соціального середовища, то існують відповідні закони щодо інформації соціального характеру, які необхідно враховувати при побудові інформаційних систем [51]. Прикладом такого закону може служити закон про захист персональних даних.

Крім приведених аргументів, при побудові інформаційних систем необхідно приймати до уваги міжнародні стандарти, які визначають вимоги до захисту інформації та вимоги з безпеки відповідної інформаційної системи. Такі вимоги є обов'язковими для врахування, оскільки вони сформовані у вигляді стандартів з безпеки інформаційних систем [52].

Стандарти, орієнтовані на розв'язання задач захисту інформаційних систем, у першу чергу, регулюють термінологію, яка використовується у галузі захисту інформації [53]. Крім того, у стандартах визначаються базові елементи, які означають компоненти, що повинні формуватися для того, щоб забезпечувати відображення всіх вимог до інформаційної системи. До таких компонентів відносяться наступні:

– задачі захисту;
– профілі захисту;
– проект захисту.

Профіль захисту представляє собою нормативний документ, який описує сукупність задач, які необхідно вирішувати в рамках інформаційної системи. Профіль захисту досить часто називають профілем безпеки системи. У ньому, крім самих задач захисту, приводяться вимоги безпеки по відношенню до визначеної категорії інформаційного продукту або інформаційної технології. Але у цьому документі не приводяться засоби реалізації необхідного захисту [54].

Проект захисту містить опис засобів захисту та обґрунтування їх використання. Структура профілю безпеки містить цілий ряд вимог, яким повинна відповідати система захисту [55]. Профіль безпеки системи, як правило, орієнтований на конкретний тип системи. Тому немає необхідності кожний раз проектувати новий профіль. Можна з бібліотеки профілів підібрати відповідний профіль і доповнити

його компонентами, які необхідні для відображення особливостей окремої системи. До основних компонентів структури профілю безпеки відносяться наступні.

Опис середовища, у якому повинна експлуатуватися система, яку передбачається захищати, складається з наступних фрагментів:

– опису основних загроз, що можуть виникати по відношенню до об’єкта, який захищається;
– політики безпеки, яка описує процес забезпечення необхідного рівня безпеки;
– умов експлуатації системи, яку прийнято називати IT-технологією.

Опис задач захисту складається з наступних компонентів:

– задачі охорони об’єкту IT;
– інші задачі захисту, які можуть розв’язуватися в рамках відповідних систем безпеки.

Опис вимог до системи безпеки складаються з наступних компонентів:

– опис вимог з функціональної безпеки системи;
– опис вимог з адекватності системи;
– опис вимог до середовища експлуатації IT;
– обґрунтування використання системи безпеки;
– обґрунтування задач захисту системи;
– обґрунтування вимог до системи безпеки.

У розділі опису загроз безпеці для кожної загрози повинні описуватися, можливі джерела такої загрози або небезпеки, яка відповідну загрозу може активізувати.

Політика безпеки описує правила безпеки, які є необхідними для забезпечення безпеки [56]. Умови експлуатації описують ті середовища, в яких буде функціонувати система з точки зору забезпечення необхідної безпеки. Задачі безпеки описують потреби користувачів, які необхідні для реалізації політики безпеки. Задачі захисту IT продукту описують всі потреби користувачів системи, які необхідні для протидії загрозам, що можуть виникати в процесі функціонування IT продукту, наприклад, необхідність в $firewall - ax, IDS$ та інші [57].

Інші задачі безпеки описують засоби протидії загрозам, які не стосуються *IT* продукту, наприклад, перепустки для користувачів і т.д. Вимоги безпеки містять описи вимог до *IT* продукту, які є необхідними для розв'язання задач безпеки. Функціональні вимоги описують умови використання конкретних методів чи засобів охорони *IT* продукту.

Вимоги адекватності описують вимоги до складу системи *IT* як з точки зору програмного забезпечення, так і з точки зору апаратних засобів, вимоги до тестування системи, вимоги до архітектури системи, вимоги до складу документації *IT* продукту та інші умови до об'єкту захисту. Обґрунтування повинно підтвердити, що вибраний профіль безпеки містить всі компоненти, які є необхідними для того, щоб *IT* продукт міг протидіяти загрозам безпеки [58]. Обґрунтування задач захисту містить аналіз, який доводить, що профіль безпеки відповідає параметрам середовища експлуатації і розв'язання задач захисту забезпечить протидію загрозам. Обґрунтування вимог до безпеки повинно підтвердити, що множина цілей, які визначені функціональними вимогами, відповідають визначеним задачам захисту. Крім того, повинно бути доведено, що вимоги безпеки не є суперечними.

1.3 Структурні підходи до методів оцінки рівня безпеки інформаційних систем

Рівень безпеки інформаційної системі типу *IS* є важливим параметром, який повинен використовуватися не тільки у певні моменти часу функціонування *IS,* а у довільні моменти часу, що визначається функціональною необхідністю отримати значення оцінки поточного стану системи. Завдяки цьому стає можливим активізувати деяку задачу в *IS* або перш ніж її активізувати, ініціювати засоби, що дозволяють підвищити поточне значення величини безпеки систем. Така необхідність може обумовлюватися не тільки потребою підвищення рівня безпеки, а також може обумовлюватися можливістю понижувати на певний період цей рівень. Необхідність пониження рівня безпеки в аспекті, наприклад, щодо полегшення доступу до системи може обумовлюватися задачами, для яких характерна висока

інтенсивність звернень до системи, що не супроводжується необхідністю забезпечувати високий рівень захисту такого доступу. Така можливість для IS може забезпечуватися різними підходами в організації системи. Прикладом такого підходу може бути структуризація даних за ознаками, що характеризують їх конфіденційність та інші.

Доцільність не тільки підвищувати, а і понижувати рівень безпеки може обумовлюватися вартістю використання засобів захисту чи пониження рівня конфіденційності даних з метою полегшення доступу до їх використання або за рахунок опосередненого знецінення тієї чи іншої інформації [59]. Прикладом останніх ситуацій можуть бути дані, що стосуються певних технологічних таємниць, а їх розсекречення може виявитися доцільним у зв'язку з необхідністю дискредитації неуповноваженої сторони, що використовує відповідну інформацію в корисних цілях і т.д.

Приведені вище фактори ілюструють доцільність включати до інформаційних систем, у тому числі, і в системи типу IS, засоби оперативного управління рівнем безпеки, що в свою чергу обумовлює необхідність володіти засобами оперативної оцінки рівня безпеки. У рамках даного підходу рівень безпеки будемо розглядати в ракурсі засобів надання повноважень, які будемо приймати як засоби захисту інформації у системі. Важливими перевагами такого підходу до управління рівнем безпеки системи є наступне:

– в рамках такого підходу знижується рівень персоналізації процесів захисту, що утруднює можливість маніпуляції з даними окремими споживачами;

– вирішення задач захисту на рівні управління повноваженнями дозволяє більшою мірою акцентувати увагу на цілях, для яких передбачається використовувати ті чи інші дані;

– такий підхід дозволяє розв'язувати задачі захисту даних способом, який полягає у їх цільовій підміні, що в свою чергу дозволяє виявляти не тільки самого інтруза, а і небезпеку, яка відповідного інтруза активізувала.

Розглянемо деякі підходи, які дозволяють в певній мірі, оперативно проводити оцінку рівня безпеки. Один із таких підходів полягає у використанні графових

структур, які відомі як дерева несправностей та дерева подій, які будемо позначати DN_i і DP, відповідно [60, 61]. Використання уявлень про DN та DP ґрунтується на тому, що такі дерева відображають процес функціонування системи. При цьому не обов'язково очікувати завершення циклу процесу для виявлення несправності, а досить провести аналіз поточного стану DN_i, що дозволяє виявити несправність, яку прийнято називати первинною, оскільки вона, відповідно до логіки функціонування системи чи її фрагменту, дозволяє перейти по відповідному дереву до несправності кінцевої або вторинної, яка проявляється своїм впливом на кінцевий етап процесу функціонування системи. Тому немає необхідності чекати кінцевого прояву виникнення несправності, а достатньо на моделі DN_i промоделювати процес розвитку первинної несправності.

У більшості випадків, всі фрагменти певного процесу можуть бути апроксимованими логічними функціями. Це означає, що така модель оперує з подіями, які відбуваються в технічній або, у даному випадку, інформаційній системі таким чином, що модель відображає факт настання події. В основному, для інформаційних систем є характерною бінарна інтерпретація їх функціонування. Це ґрунтується на тому, що у довільній системі процеси, які реалізуються в окремих фрагментах, на інших етапах функціонування допускають інтерпретацію повстання або не повстання деякої події [62].

У рамках такого підходу можна визначити наступні положення, які визначають аналітичні можливості моделі DN і DP.

Положення 1.1. Окремі фрагменти функціонування системи представляються таким чином, що існує можливість детерміновано описувати функціонування на одному етапі такого процесу.

Наприклад, якщо фрагмент φ_i відображає адекватно процес функціонування, то існує логічна формула $\varphi_i(a_i) \to L_i\left(a_i^B\right)$, яка його описує. У багатьох випадках описи окремих фрагментів певного процесу не дозволяють однозначно стверджувати, що в результаті виконання фрагменту $\varphi(x_i)$ виникне деяка подія. У таких випадках використовуються ймовірнісні оцінки можливості виникнення деякого результату функціонування відповідного фрагменту. У цьому випадку виникнення події

визначається деякою ймовірною величиною, яку будемо описувати у загально прийнятому вигляді $P_i(x_i)$, де $P_i(x_i)$ означає деяку ймовірність виникнення події x_i в результаті функціонування фрагменту процесу φ_i. У рамках таких моделей для їх формального опису використовується логічні функції & та V, як основні компоненти та цілий ряд різновидностей функцій логічного типу, які допускають свою інтерпретацію в бінарній множині [63]. Наприклад, у логічному операторі виключаючої диз'юнкції вихід такої функції може приймати одне з бінарних значень, наприклад «1», лише у тому випадку, коли тільки на одному з входів появилася подія, яка інтерпретується значенням «1». На відміну від класичної диз'юнкції V, яка допускає появу "1" на виході, коли на двох її входах є одиниці, тому, будемо використовувати для позначення виключаючої дизюнкції символ "U". Залежно від потреб, що визначаються особливостями системи та особливостями задач, які реалізуються, можна вводити цілий ряд інших операторів, що допускають бінарну інтерпретацію [64].

Оскільки дерево подій на початковому етапі будується на основі інтерпретації інформаційної системи та на основі інтерпретації окремих задач, що розв'язуються в рамках системи, то відповідне дерево подій може виявлятися надмірним [65]. У цьому випадку розв'язується задача оптимізації такого дерева, що дозволить скоротити час його аналізу. Один з таких методів полягає у визначенні найменшого перерізу дерева подій (рис. 1.1).

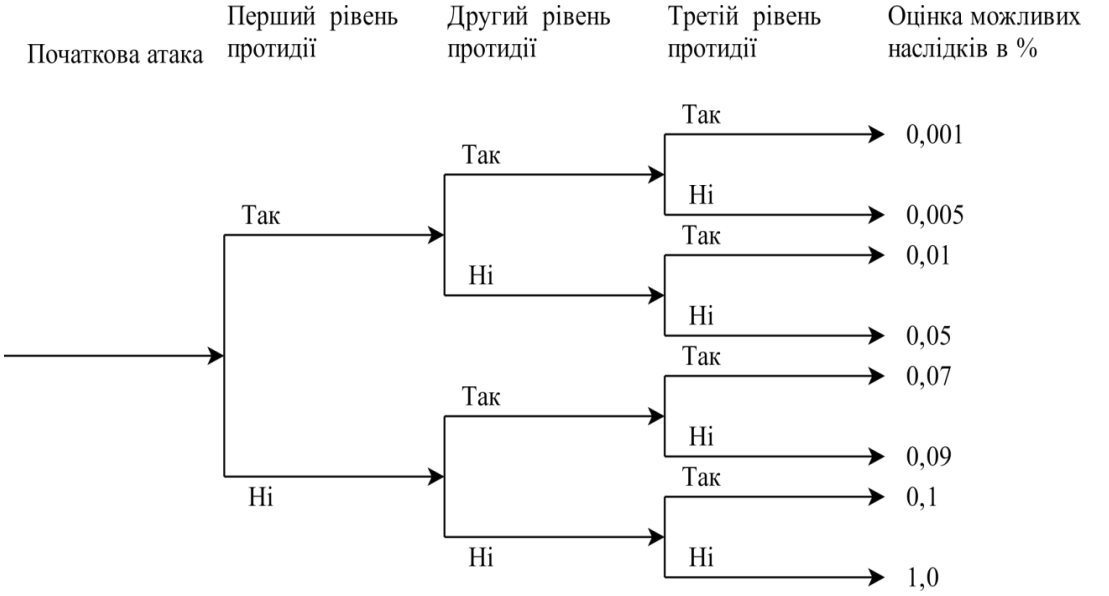

Рис. 1.1. Дерево подій

У межах булевої алгебри визначення найменшого перерізу ґрунтується на мінімізації булевої формули, що описує відповідне дерево. Для ілюстрації цього методу пошуку найменшого перерізу DP приймемо, що кінцева подія описується булевою формулою $f(x_1, x_2, x_3, x_4)$. Відповідно до вибраної для прикладу структури розв'язання задачі виявлення $f(x_1x_2, x_3, x_4)$ таку структуру можна описати логічною формулою:

$$f(x_1, x_2, x_3, x_4) = (x_1 + x_2)(x_1 + x_3) + (x_1 + x_4) \cdot x_1 + x_1 \cdot x_3 \quad (1.2).$$

За допомогою відомих правил перетворень:

1) $z \cdot (x + y) = x \cdot z + y \cdot z$;

2) $x + x = x$;

3) $x \cdot x = x$,

приведену формулу для $f(x_1, x_2, x_3, x_4)$ можна перетворити у вираз:

$$f(x_1, x_2, x_3, x_4) = x_1 + x_2 \cdot x_3 + x_2 \cdot x_4$$

Цей вираз описує мінімальну логічну залежність, яка відображає залежність вихідної події $f(x_1, x_2, x_3, x_4)$ від вхідних події x_1, x_2, x_3x_4. Відповідно до отриманого опису мінімального перетину дерева DP, кінцева подія може виникнути в наступних випадках:

– при появі події x_1,
– при появі подій x_2 і x_3,
– при появі подій x_2 і x_4.

У результаті визначення мінімального перерізу дерева подій, в рамках конкретної задачі, можна перейти, до структури дерева, яке не має надмірності. Слід зауважити, що при переході до іншої задачі, необхідно повернутися до початкового дерева, оскільки в цьому випадку можуть появитися нові вхідні величини та може змінитися основна вхідна подія.

Використання дерев типу DN і DP дозволяє проводити аналіз безпеки системи не тільки у випадку детермінованих подій у процесах, що описуються деревами, а і у випадку, коли події, які описуються, носять ймовірнісний характер. В багатьох випадках буває досить складно привести систему до ситуації, коли її можна було б описувати детермінованими співвідношеннями. Для можливості проведення

ймовірнісного аналізу процесів на основі використання дерев несправностей та дерев подій, необхідно пов'язати ймовірності з логічними елементами, що використовуються для побудови DN і DP. Розглянемо таку інтерпретацію на прикладі операції кон'юнкції та диз'юнкції. Для випадку операцій кон'юнкції ймовірність виникнення події на виході, при відомих ймовірностях виникнення вхідних даних, описується наступним співвідношенням:

$$\rho(a, b, \ldots, c) = \rho(a) \cdot \rho(b) \cdot, \ldots, \cdot \rho(c)$$

Приведена інтерпретація є досить простою і очевидною. Для випадку операції диз'юнкції, коли вхідні події є не залежними, ймовірність появи вихідної події описується співвідношенням:

$$\rho(a, b, \ldots, c) = \rho(a) + \rho(b) + \ldots + \rho(c) \qquad (1.3)$$

З точки зору принципів оцінки ймовірнісних подій, для диз'юнкцій з двома входами, ймовірність вихідної події описується співвідношенням:

$$\rho(a, b) = \rho(a) + \rho(b) - \rho(a \cdot b)$$

У випадку, коли a і b статистично незалежні і добуток $\rho(a) \cdot \rho(b)$ досить малий, то $\rho(a, b) \approx \rho(a) + \rho(b)$, що обумовлює коректність використання співвідношення (1.3).

На основі використання моделей, що ґрунтуються на уявленнях про дерева несправностей та дерева подій, можна розв'язувати цілий ряд задач, які в тій чи іншій мірі, допускають інтерпретацію забезпечення того чи іншого рівня безпеки. До таких задач відносяться:

– задача оцінки інтенсивності успішності атак;

– задача оцінки безпеки при відновленні елементів, що були дискредитовані успішними атаками;

– задача оцінки безпеки при дії масових атак та інші.

На основі розв'язання приведених вище задач можна проводити узагальнені оцінки рівнів безпеки, які мають власні та досить специфічні інтерпретації. Першою з таких є оцінка по Бірнбауму [66]. Важливість події x по Бірнбауму визначається відношенням зміни частоти успішних атак до зміни ймовірності реалізації події x, що формально описується наступним співвідношенням:

$B(x) = \frac{d}{dx}[P(x)]; B(x) = F(1) - F(0).$

Величина оцінки по Бірнбауму представляє собою різницю між частотою успішних атак при виникненні події x і частотою успішних атак у випадку, коли подія x не виникла. Коефіцієнт збільшення величини ризику (RIR) показує як збільшується мінімальна верхня границя мінімальних перетинів коли ймовірність головної події збільшується і прямує до одиниці:

$$RIR = F(\lambda)/F(x).$$

Значимість по Фуселу-Веселу події x визначається як відносний вклад події в частоту успішних атак:

$Fv = [F(x) - F(0)]/F(x)$,

де $F(x)$ – частота успішних атак при номінальному значенні ймовірності основного значення x; $F(0)$ – те ж саме, але при припущенні, що подія x не виникла.

Алгоритм обчислення величини ризику системи може полягати у наступній послідовності дій.

Ризик буде обчислюватися для окремих задач, оскільки користувача цікавить безпека співпраці з мережею в аспекті задачі, яку користувач використовує.

Кожна задача описується у вигляді дерева подій DP, множина яких описує відповідну роботу користувача.

Для всіх відомих несправностей (по відношенню до всіх станів в DP) будується дерево несправностей або відмов (DN) (рис 1.2).

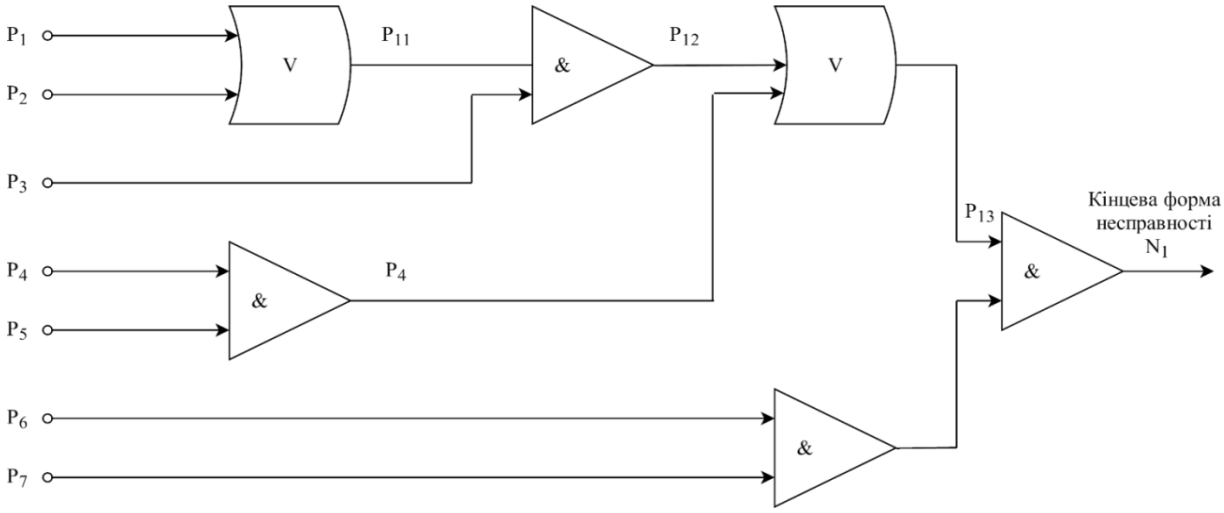

Рис. 1.2. Дерево несправностей

На основі емпіричних даних обчислюється ймовірність переходу з одного стану до іншого при виникненні відповідних подій.

Базовим співвідношення для оцінки інтенсивності потоку несправностей або відмов є співвідношення Пуассона:

$P(x,t) = \left(\lambda^x \cdot e^{-\lambda}\right)/x!$, де λ – інтенсивність відмов. Середнє значення частоти рівне $\lambda = x/t$, де x – кількість відмов за час спостереження t. Для рідких подій, в якості середнього значення приймається оцінка $\lambda = 0{,}693/t$. Довірена границя у випадку Пуассоновських відмов визначається у відповідності із співвідношенням:

$\lambda_\alpha = -\ln(1-\alpha)/t$, де α – довірена границя ймовірностей.

Поточна у часі величина ризику локальної мережі по Бірнбауму обчислюється співвідношенням:

$$R(S) = \sum_{j=1}^{n}\sum_{i=1}^{k} RIR_j(x_i)$$

У процесі функціонування мережі, змінюється значення ймовірності $P_i(x_i)$ подій, які виникають в мережі і відображаються в DP. Залежно від виникнення атак різних типів, змінюються значення x_i в DN. Тому змінюються характеристики ризику по Бірнбауму в локальній мережі.

Для визначення рівнів безпеки можна використовувати методи, що будуються на основі Марківських моделей. Марківський процес – це процес, у якого кожний наступний стан системи залежить тільки від стану системи в момент часу t_{i-1}. Введемо наступні позначення:

– "0" $-$ "l" - безпечні стани мережі;
– "1.1" $-$ "$n.1$" - небезпечні стани мережі;
– $\lambda_{1.0} - \lambda_{n.1}$ - інтенсивності переходів у відповідні стани;
– $\mu_1 - \mu_l$ - інтенсивності переходів з безпечних станів в інші безпечні стани.

Інтенсивність переходів в стан "$i.0$" описуються співвідношенням $\lambda_{i.0}(i) = \lambda_i(t) \cdot Q_i(t, t_p)$, де λ – інтенсивність переходу з і-го початкового стану, $Q_i(t, t_p)$ – ймовірність виконання всіх функцій захисту в і-тому початковому стані. Інтенсивність переходу стану "$i.1$" з порушенням безпеки при і-тому початковому

стані описується наступним чином: $\lambda_{i,1}(t) = \lambda_i(t)Q(t, t_p)$, де $Q(t, t_p)$ – ймовірність не виконання функції забезпечення безпеки.

Для можливості використання зазначеного підходу до моделювання рівня безпеки, з метою оперативного визначення цього рівня, необхідно представити задачі, що розв'язуються в цій системі у вигляді окремих станів систем і переходів системи з одного стану в інший стан.

Оскільки в рамках даної роботи розглядаються інформаційні системи і в першу чергу, програмні засоби, які реалізують такі системи, тому доцільно розглядати параметри, що пов'язані з надійністю системи, оскільки остання, як і безпека, визначається як параметр, що характеризує здатність системи розв'язувати задачі, що передбачені технічними умовами на відповідну систему. Якщо розглядати надійність IS на зальному рівні, то можна стверджувати, що безпеку системи можна, в певній мірі, пов'язати з надійністю. Атаки, що скеровуються зовнішніми небезпеками на систему, можуть мати вищу успішність, якщо система містить в програмному середовищі похибки, які не вдалося виявити на етапах проектування та випробування системи. Одним з базових підходів до підвищення надійності системи є перевірка її відповідності встановленим вимогам. Одним з основних підходів до реалізації таких перевірок є тестування системи програмних засобів. Атаки, що активізуються зовнішніми небезпеками, в більшості випадків, ґрунтуються на даних про систему. Тому такі данні про небезпеку, якою найчастіше виступає деяка зовнішня інформаційна система, проводить дослідження IS. У результаті використання таких даних небезпека може сформувати більш ефективну атаку. Таке дослідження може представляти собою тестування потенціального об'єкту атаки з метою виявлення слабких місць і по можливості дефектів, які могли залишитися після розробки та випробування IS [67]. У цьому випадку функції захисту в системі понині бути розширені засобами, що виявляють відповідні спроби несанкціонованого дослідження системи. Функції дослідження системи IS можуть реалізовуватися на рівні доступу до системи надання повноважень. Тому доцільно розглянути модель надійності системи програм, яка вносить свою частку в рівень безпеки відповідної системи [68]. У зв'язку з цим розглянемо деякі моделі

надійності, а також можливість їх інтерпретації з точки зору забезпечення та оцінки рівня безпеки інформаційної системи.

Одним з підходів до визначення рівня надійності інформаційної системи є підхід, що ґрунтується на оцінці можливих помилок, які могли залишитися в програмному середовищі. Тоді показником надійності програмного забезпечення служить ймовірність відсутності програмних помилок протягом певного інтервалу часу експлуатації відповідної програми [69]. Одна з таких моделей ґрунтується на наступних припущеннях:

– загальна кількість операторів в програмі є постійна;

– в процесі відладки інформаційної системи певна кількість помилок виявляється та усувається, при цьому до системи не вносяться нові похибки;

– за сумарною кількістю виявлених помилок можна проводити оцінку кількості помилок, що залишилися;

– інтенсивність відмов системи пропорційна числу помилок, що залишилися.

В даному випадку надійність системи визначається величиною середнього періоду часу безвідмовності роботи системи, який визначається співвідношенням наступного типу:

$$T_0 = 1\big(K_s\big[E_0\big(1 - e_c(x)\big)\big]\big),$$

де K_s і E_0 – параметри моделі надійності; $e_c(x)$ – сумарна кількість помилок, що виправлені до моменту t; I – загальна кількість операторів у системі на момент часу t_0. Параметр E_0 визначається співвідношенням:

$$E_0 = \{I[\gamma e_c(x_1) - e_c(x_2)]\}/(\gamma - 1), \text{ де } \gamma = (T_1/T_2) * (n_2/n_1) = T_{01}/T_{02},$$

де T_{01} - середній час безвідмовної роботи, який відповідає періоду відладки системи і позначається x_i. Тоді $T_{0i} = T_i/n_i$, де n_i – поточне число помилок у системі, що були виявлені у процесі відладки за період x_i. Параметр K_s обчислюється за наступною формулою:

$$K_s = n_1/\{[(E_0/I) - e_c(x_1)]T_1\},$$

де T_1 і T_2 - час роботи системи, який відповідає інтервалам часу x_1 і x_2.

Наступна модель надійності програмної системи, як і попередня, ґрунтується на припущенні про експоненціальний розподіл часу безпомилкової роботи програмної

системи. Приймається, що частота появи помилок пропорційна числу помилок, що залишилися [70]. Тоді середній час безпомилкової роботи системи визначається наступним співвідношенням:

$$T_0 = 1/\{K_{JM}[E_0 - i + 1]\},$$

де K_{JM} – коефіцієнт пропорційності; і – номер поточного інтервалу, що визначає період, через який була виявлена поточна помилка; E_0 – число помилок, що існують в програмі на початковому моменті x_0.

Наступна модель надійності програми відрізняється від попередніх тим, що припускається наступне. Частота появи помилок пропорційна не тільки кількості помилок, що залишилися, а і часу відладки програми. Така модель описується наступним співвідношенням:

$$T_0 = \left\{[\pi/2K_{SW}(E_0 - i + 1)]^{1/2} = \sqrt{\pi/2|K_{SW}(E_0 - i + 1)}\right\},$$

де T_0 – час роботи або інтервал часу роботи, який програма буде працювати без помилок; K_{SW} – коефіцієнт пропорційності.

На рівень безпеки інформаційної моделі впливає цілий ряд факторів. До них відносяться:

– модульність інформаційної системи;
– модифікація програмних засобів в процесі експлуатації інформаційної системи;
– періоди експлуатації системи та інші.

Це призвело до того, що вводяться уявлення про нескінченні моделі надійності, оскільки кількість помилок у програмі може бути нескінченна. Це пов’язано з тим, що при усуненні одних помилок можуть виникати нові. Систематична модифікація програми також призводить до можливості появи нових помилок і т.д. Тому крім загально прийнятих початкових умов, вводиться положення про те, що накопичена кількість помилок в програмі у поточний момент t описується процесом Пуассона з середнім значенням його величини, яка описується співвідношенням: $\mu(t) = \alpha t^{\beta}$, де оцінки α і β визначаються наступними співвідношеннями:

$$n/t^{\beta}; \beta = n/[\sum_{i=1}^{n-1} \ln(t_n/t_1)].$$

Приведена модель є більш близька до моделі визначення рівня безпеки, яка повинна враховувати вторгнення до системи атак.

Припущення про те, що нові помилки можуть вводитися до системи, досить добре підходить для випадків, коли атака, реалізація якої представляє собою програмний продукт, вторгається в систему. Цей факт допускає інтерпретацію, що полягає в наступному. Будь-яке вторгнення програмного інтруза до системи приводить до ефектів, які відповідають наслідкам активізації фрагментів програм, що містить помилки.

При цьому у випадку атак, які полягають у внесенні змін до програм, можуть виявлятися не відразу, що не відповідає у більшості випадків прояву звичайних помилок в інформаційній системі.

Приведені моделі надійності можуть використовуватися певною мірою, як доповнення реалізації моделей безпеки інформаційної системи. При цьому, можна приймати положення, що допускають інтерпретації ситуацій, які виникають, при появі атаки, що здійснила вторгнення в середовище програмної системи.

Висновок до розділу 1

У першому розділі проводиться аналіз відомих методів надання повноважень користувачу на використання даних, що знаходяться в інформаційній системі. Один з поширених методів надання повноважень ґрунтується на використанні матричних моделей. У рамках такої матриці існує можливість зіставляти кожному з користувачів певні об’єкти, якими є дані, програми чи процеси, до яких цей користувач може мати відповідні повноваження. Прикладом таких повноважень можуть бути повноваження на виконання операцій читання, запису, заміни інформації та інші. Відомими є моделі надання повноважень, які використовують уявлення про класи безпеки та уявлення про категорії об’єктів.

Проводиться також аналіз методів оцінки рівня безпеки, оскільки необхідно мати можливість кількісно оцінювати небезпеку і, відповідно, необхідний рівень безпеки, яка забезпечується певними засобами захисту системи. Однією з поширених оцінок є оцінка, яка використовує уявлення про ризик зниження рівня безпеки системи. Також широко використовуються методи, що ґрунтуються на

використанні експертних оцінок. У більшості з них, в якості експертів використовуються фахівці, які можуть оцінити рівень вразливості окремих засобів, можливість виникнення загрози та інші фактори. Всі ці оцінки представляються у вигляді певної таблиці, до якої впроваджуються правила її використання, що використовуються при визначенні рівня ризику.

Для оцінки рівня безпеки досить широко використовуються структурні методи, які ґрунтуються на використанні деревоподібних графів, що відображають послідовність подій, які можуть виникати в системі внаслідок дії на систему зовнішніх негативних факторів. Крім цього, використовуються дерева несправностей, які відображають процеси виникнення та розвитку несправностей, що обумовлюються дією на систему негативних факторів.

Приведений аналіз ілюструє необхідність розвитку методів надання повноважень, які забезпечували б необхідний рівень безпеки інформаційної системи.

РОЗДІЛ 2 Дослідження методів формального опису процесів надання повноважень

2.1 Використання формальних засобів опису параметрів процесів надання повноважень

Системи надання повноважень можуть мати різноманітну інтерпретацію, починаючи від представлення їх у вигляді матриць повноважень до приписування тих чи інших ролей користувачам, які звертаються за наданням повноважень. Це свідчить про те, що для формального опису самих систем можна використовувати досить широкий спектр формальних засобів [71]. Для того, щоб використовувати найбільш адекватні формальні засоби відносно інформаційних систем типу IS, необхідно провести детальний аналіз параметрів, що характеризують систему.

Перший параметр або перша особливість полягає у залежності між рівнем конфіденційності даних та кількістю користувачів, які можуть такими даними користуватися. Якщо позначити кількість користувачів h_i, що звертаються за даними x_i символом m, а рівень конфіденційності даних x_i позначити $r_i(x_i)$, то можна записати наступну залежність:

$r_i(x_i) = k_{Rz}/mh_i(\alpha)$ (2.1),

де m – кількість користувачів h_i, кожний з яких може мати певний рівень власного рівня безпеки, яка описується величиною, $\alpha, 0 \prec \alpha \leq 1, k_{Rz}$ – коефіцієнт пропорціональності, який визначає рівень максимального рівня конфіденційності. Якщо $\alpha = 1$ і $m = 1$, то $r_i(x_i) = \max r_i(x_i) = K_{RZ}$. Використання коефіцієнта α дозволяє представити величину зміни рівня захищеності як неперервну величину, яка може приймати проміжні значення між дискретними значеннями рівня конфіденційності. Коефіцієнт α може використовуватися лише в тому випадку, коли кількість користувачів $m \succ \beta$, де, наприклад, $\beta \succ 4$. Загалом, можна написати наступну умову, якій повинна задовольняти величина α: $\sum_{n=1}^{m} h_i(\alpha) \geq 1$. Формулу (2.1) можна записати у наступному вигляді:

$r_i(x_i) = k_{RZ}/\sum_{i=1}^{m} h_i(\alpha_i)$ (2.2)

Виходячи з цієї особливості може скластися враження, що необхідний рівень конфіденційності $r_i(x_i)$ може визначатися кількістю користувачів і не залежати від інших факторів, наприклад, рівня небезпеки пониження рівня конфіденційності. Цей фактор, у рамках даного підходу, також пов'язується з користувачем за рахунок використання параметра α_i. Цей параметр представляє собою дробову величину, врахування якої призводить до того, що використання даних x_i користувачем $h_i\alpha$, якщо $\alpha \neq 1$ обумовлює зростання рівня захищеності, який стає більшим K_{RZ} або $r_i(x_i) \succ K_{RZ}$. З точки зору інтерпретації співвідношення (2.1) це означає наступне. Якщо $\alpha_i = 0{,}5$ для h_i, то особистий параметр, що характеризує пониження рівня безпеки через надання h_i даних x_i, характеризує властивість самого користувача, який може інформацію про ці дані розповсюдити між іншими користувачами, які можуть бути не уповноваженими до отримання даної інформації. Таким чином, якщо виявиться, що у відповідності з (2.1) або з (2.2) встановлений рівень конфіденційності з допомогою коефіцієнта K_{RZ} зріс, цей факт має знайти своє відображення в засобах захисту [72], які повинні такий рівень захисту для x_i збільшити. Формально це можна описати у вигляді наступного логічного співвідношення зростання конфіденційності:

$$\{[K_{RZ}/h_i(\alpha_i)] \rightarrow (K^*_{RZ} \succ K_{RZ})\} \rightarrow \left[r_i(x_i) \rightarrow \left[r_i^*(x_i) = [K^*_{RZ}/h_i(\alpha_i)]\right]\right].$$

Приведене співвідношення описує зміни, які повинні відбутися в системі надання повноважень (SNP), якщо виникає ситуація, коли h_i має доступ до даних x_i, але його характеристика власного рівня безпеки α_i, яка задається в рамках самої системи IS, не надає йому змоги отримати повноваження на виконання певних дій з даними x_i, що мають рівень конфіденційності $r_i(x_i)$.

Друга особливість полягає у тому, що рівень конфіденційності з часом зменшується залежно від того, які дії чи зміни відбуваються з x_i [73]. Якщо x_i використовуються часто, то таке зменшення $r_i(x_i)$ протікає у часі швидше, якщо x_i використовується не часто, то зміни відбуваються повільніше. Якщо x_i взагалі не використовується, то зміна значення $r_i(x_i)$ може відбутися раптово через певний проміжок часу. Формально це описується наступними співвідношеннями:

$$\{(m(x_i) = 0)\&(\delta t_i(x_i)) \geq \Delta T_i(x_i)\} \rightarrow [(r_i(x_i) = 0)\&(x_i \notin IS)]$$

$$[(m(x_i)/\Delta t) \rightarrow 0] \rightarrow [r_i(x_i) \rightarrow \min r_i(x_i)] \qquad (2.3)$$

Приведена особливість, як і особливість попередня, визначає рівень конфіденційності або $r_i(x_i)$ незалежно від абсолютної вартості даних x_i. Говорити про такого типу вартість даних є сенс лише у тому випадку, коли можуть виникнути задачі, для розв'язання яких можуть виявитися відповідні дані необхідними. Для встановлення таких фактів, необхідно проводити аналіз описів інтерпретації відповідних даних. Приймається, що тільки такий опис повністю може описувати рівень активності даних, а також рівень їх значимості, пов'язаний з рівнем $r_i(x_i)$. Інтерпретаційний опис даних представляє собою наступне формальне представлення x_i, що описується співвідношенням:

$$j(x_i) =< a_{i1} * \ldots a_{in} > I < \lambda_{i1}, \ldots, \lambda_{im} >,$$

де a_{ij} – окремі фрази чи слова на мові користувача, які в сукупності, у відповідності з граматикою відповідної мови, описують повною мірою величину x_i, яка фактично є лише ідентифікатором $j(x_i)$, λ_{ij} – параметри, які використовуються для доповнення інтерпретаційного опису, що формується за допомогою $a_{i1}, \ldots, a_{in}$. Будь-який інтерпретаційний опис $j(x_i)$ може бути не повним. На момент формування IS приймається, що $j(x_i)$ є повним у рамках задач, на які орієнтована система IS. Це означає, що система надання повноважень SNP може використовувати також $j(x_i)$ відповідні дані, які користувач передбачає використовувати для розв'язання задач.

У відповідності зі співвідношенням (2.3), $r_i(x_i) \rightarrow \min\ r_i(x_i)$, якщо кількість запитів x_i зменшується або зменшується інтенсивність цих запитів, що не до кінця повно відображає досліджуваний фактор. Тому введемо наступне положення.

Положення 2.1. Рівень конфіденційності відповідних даних x_i з часом зменшується незалежно від інтенсивності використання x_i для розв'язання задач.

У зв'язку з цим виникає необхідність розділити уявлення про значимість даних x_i та рівень їх конфіденційності. Розглянемо наступні визначення, яких будемо дотримуватися в рамках даної роботи.

Визначення 2.1. Важливістю даних x_i будемо називати параметр, що характеризує частоту використання даних за період часу, протягом якого відповідні дані використовуються. Формально це визначення описується співвідношеннями:

$$\aleph(x_i) = \left[m_j(x_i)/\Delta t_j\right],$$

де $\aleph(x_i)$ – значимість даних, що ідентифікуються змінною $x_{i,}$ m_j – кількість запитів на використання даних x_i за встановлений проміжок Δt_i [74].

Визначення 2.2. Рівень конфіденційності $r_i(x_i)$ даних x_i зв'язаний з рівнем небезпеки, до якої може привести несанкціоноване використання x_i під час розв'язання задачі $Za_i(x_i)$.

Рівень небезпеки, який будемо позначати символами nb_i, визначається для середовища, в рамках якого описується ціль $c_i(z_i)$ задачі $z_i(x_i)$. Рівень небезпеки $nb_i(x_i)$ не означає, що цей рівень безпосередньо визначає рівень конфіденційності $r(x_i)$. Це зв'язано з тим, що визначення міри небезпеки розв'язання несанкціонованої задачі, яка використовує дані x_i для певної предметної області, представляє собою досить складну задачу, в якій необхідно враховувати цілий ряд факторів та їх різні інтерпретації. Тому у більшості випадків оцінка $nb_i(x_i)$ проводиться експертним способом. В якості експерта обирається фахівець, обізнаний з відповідною предметною областю, у якій розв'язується задача [75]. Відповідний експерт на основі представленої шкали рівнів конфіденційності визначає величину $r_i(x_i)$ в IS. Якщо IS використовується в різних предметних областях W_i, то $r_i(x_i)$ вибирається по тій предметній області W_i, для якої величина $r_i(x_i)$ є максимальна. Зниження рівня конфіденційності $r_i(x_i)$ з часом її існування будемо називати старінням параметру $r_i(x_i)$. Зниження рівня значимості $\aleph(x_i)$ з часом також будемо називати старінням даних x_i. Процес старіння в одному і другому випадках будемо позначати символом S і формально цей процес будемо описувати наступними співвідношеннями: $S[r(x_i)] = f_r\left(m_i(x_i), \Delta T(x_i)\right)$.

Для випадку старіння значимості даних $\aleph(x_i)$ відповідний вираз у неявній формі записується аналогічно: $S[\aleph(x_i)] = f_\aleph\left(m_i(t_i)\right)$. Оскільки старіння $r_i(x_i)$ та

$\aleph(x_i)$ представляють собою процеси, то необхідно описати логіку перебігу цих процесів. Такий опис представляє собою наступні співвідношення:

$$[r(x_i)\&(\Delta t_i(x_i) \to \Delta T_i)] \to [(r(x_i) \to 0)]$$

$$[\aleph(x_i)\&(m(x_i) \to 0)] \to (\aleph(x_i) \to 0)$$

Очевидно, що ці співвідношення можна представити в аналітичній формі, але ця форма буде залежати від W_i та інших факторів. Тому в даному випадку не будемо їх формувати. Задачі, що розв'язуються на основі використання даних IS, тісно пов'язані не тільки з установою, яка є власником IS, а із параметрами, що характеризують $x_i \in IS$. Одним з таких параметрів є параметр конфіденційності $r(x_i)$. У найпростішому випадку такий зв'язок представляє безпосередню залежність між $r(x_i)$ та $r[z_i(x)]$, яка представляє собою наступне:

$$[r(x_i)\&(x_i)] \to \{(r(x_i)) = r[z(x_i)]\}.$$

Такий підхід не є оптимальним, оскільки він призводить до необхідності надавати величині $r(x_j)$, де $x_j \in IS$ – значення конфіденційності задачі, якщо $x_j \in z(x_i, x_j)$. Оскільки в рамках $z_i(IS)$ можуть існувати запити не тільки на дані, а і на процеси, які будемо позначати $y_i = e(x_{i1}, \ldots, x_{im})$, то і відповідні процеси, які використовують x_i з $r_i(x_i)$, також повинні отримувати відповідний рівень конфіденційності. Якщо $r(z_i(x_i)) \prec r(x_i)$, то вся задача або фрагмент задачі, у якому використовується x_i, передається для розв'язання до засобів IS. Крім того, система SNP розв'язує задачу визначення можливості тимчасового пониження $r_i(x_i)$ до $r_i^*(x_i)$, де $r * (x_i) \prec r(x_i)$, яке можливе за рахунок того, що дані, які отримані в результаті розв'язання задачі $z(x_i, \ldots, x_k)$ не розкривають або не понижують конфіденційності $r(x_i)$. Ця задача зводиться до аналізу рівня оберненості алгоритму, який використовує $z(x_i, \ldots, x_k)$. Це не означає, що SNP повинна проводити цей аналіз самостійно. Достатньо щоб користувач при зверненні за повноваженнями щодо $x_{i,}$ надавав системі відповідну інформацію. Це означає, що SNP повинна використовувати не тільки інформацію, що характеризує задачі, а і інформацію, яка стосується алгоритму самої задачі z_i. Важливими даними, що використовуються SNP, є дані про задачу, які полягають у наступному:

– мета розв’язання задачі $c(z_i)$;

– наявність повноважень у h_i на розв’язання z_i;

– параметри задачі z_i;

– інші зовнішні засоби, які повинна використовувати задача z_i в процесі розвязку;

– додаткові параметри, що можуть стосуватися користувача відповідної задачі.

Мета розв’язання задачі оцінюється окремими параметрами, які приписуються їй незалежно від IS з якою ця задача передбачає співпрацювати. Параметри мети визначаються на основі W_i в рамках якої розв’язується задача. Прикладом таких параметрів можуть служити: рівень конфіденційності мети $r\big(c_i(z_i)\big)$, рівень значимості мети $\aleph[c_i(z_i)]$, рівень відповідності предметної області мети задачі $W_i[c_i(z_i)]$ предметної області W_i, на обслуговування якої орієнтована IS або $W_j(IS)$. Очевидно, що IS може бути орієнтована на цілий ряд предметних областей або $IS_i(W_i, W_{i+1}, \dots, W_m)$. Наявність повноважень у h_i є додатковими характеристиками користувача, які не пов’язані безпосередньо з ідентифікацією та автентифікацією користувача. Повноваження користувача $p(h_i)$ визначаються наступними параметрами задачі:

– рівнем конфіденційності задачі $r_i(Za_i)$;

– рівнем значимості задачі $\aleph(Za_i)$;

– параметрами, що характеризують ціль задачі $p[C(Za_i)]$;

– рівнем актуальності задачі для $W_i(IS)$, якщо основна предметна область інтерпретації задачі $W_j \neq W_i$, яку будемо позначати $A[Z_i(W_i)]$;

– кількість конфіденційних даних, які використовуються у задачі, що мають високі рівні конфіденційності з вибраного діапазону цих рівнів $kr_i(x_i, \dots, x_n)$.

Формально це можна записати у вигляді:

$p(z_i)=f\{r_i(Za_i), p[C(Za_i)], \aleph_i(Za_i), A[Z_i(W_i)], kr_i(x_1, \dots, x_n)\}$.

Параметр $p(h_i)$ не мусить бути залежним від усіх компонент. У випадку, коли параметр $p[c(z_i)]$ відповідає рівню конфіденційності мети $r[c(z_i)]$, існує можливість співставити його з $r(x_i)$, який передбачається використовувати для

розв'язання задачі z_i. Аналогічно актуальність задачі можна привести до параметра значимості задачі. Приведені випадки записуються у вигляді:

$$p[c(z_i)] \to r[c(z_i)] \to r(x_i, \dots, x_m);$$

$$a[z_i(W_i)] \to \aleph(Za_i)$$

Параметр $kr_i(x_i, \dots, x_n)$ є більш складним. Ця складність обумовлюється тим, що не допустимо при визначенні рівня конфіденційності встановлювати між ними лінійну залежність, а спільне використання різних x_i, x_j, x_k з найвищими рівнями конфіденційності $r_i(x_i), r_j(x_j), r_k(x_k)$ не обов'язково призводить до того, що $r_e(x_e) = F(x_i, x_j, x_k)$ буде приймати максимальне значення рівня конфіденційності з уже встановлених рівнів. Формально це описується наступним співвідношенням:

$$\{r_e(x_e) = Ae[r_i(x_i), r_j(x_j), r_k(x_k)]\} \to \{\{r_e(x_e) = \max[r_i(x_i), r_j(x_j), r_k(x_k)]\} V$$

$$\{[r_e(x_e) \succ \max(r_i(x_i), r_j(x_j), r_k(x_k))] \, v \, [r_e(x_e) \prec \max(r_i(x_i), r_j(x_j), r_k(x_k))]\}\}$$

Співвідношення $r_e(x_e) = \max[r_i(x_i), r_j(x_j), r_k(x_k)]$ відповідає присвоєнню максимального рівня конфіденційності результату перетворень $F[r_i(x_i), r_j(x_j), r_k(x_k)]$. Алгоритм Ae_i вибирає серед заданих для x_i, x_j, x_k рівнів конфіденційності той рівень, який відповідає виразу $r_e(x_e) = [r_i(x_i), r_j(x_j), r_k(x_k)]$. Ситуація, коли рівень конфіденційності $r_e(x_e) \succ \max[r_i(x_i), r_j(x_j), r_k(x_k)]$ є більш складна і потребує більш детального аналізу. Рівень конфіденційності в IS визначаються не тільки для даних, а й для фрагментів алгоритмів, які можна вважати окремими функціями, що використовуються в рамках розв'язання задач доступу і, в першу чергу, в рамках розв'язання задач надання повноважень користувачам в IS. Такі функції будемо називати φ_i функціями. Система рівнів конфіденційності $R\{r_i, \dots, r_m\}$ та система значимостей $\Im\{\aleph_1, \dots, \aleph n\}$ визначаються на основі використання описів текстових інтерпретацій всіх даних $j(x_1), \dots, j(x_n)$, які розміщаються в IS та на основі аналізу текстових описів інтерпретацій елементів бібліотеки всіх функцій $\varphi_i = \{j(\varphi_1), \dots, j(\varphi_k)\}$. Основою для цього є опис інтерпретації предметних областей, до яких відносяться IS або $W_i(IS)$. Для вирішення задачі визначення рівнів конфіденційності та значимості

використовуються критерії для r_i та $\aleph_i$, а процеси визначення конкретних значень $r_i(x_i)$ та $\aleph_i(x_i)$ реалізуються шляхом використання семантичного аналізу [75]. У даному випадку розглянемо задачу, яка полягає у визначенні рівня конфіденційності r_i, який є вищий від встановлених рівнів конфіденційності при формуванні IS для даних $x_i \in IS$ та $\varphi_i \in IS$.

Перш ніж доводити можливість виникнення необхідності приведення рівня конфіденційності $r_i(x_i) \succ r_j(x_j)$ до $r_j(x_j) = \max$, розглянемо цю ситуацію на якісному рівні. Уявлення про конфіденційність r_i тих чи інших даних є необхідним лише для того, щоб не допустити можливих аномалій на деякому фрагменті $W_i(IS)$. Введемо визначення аномалії для W_i.

Визначення 2.3. Аномалією An_i в W_i називаються наступні ситуації, що можуть виникати в W_i:

– виникнення структурної суперечності в W_i;
– виникнення логічної суперечності в W_i;
– виникнення семантичної суперечності в W_i.

Структурна суперечність відповідає такій ситуації, коли в рамках структури W_i не може бути розв'язана задача, яка на структурному рівні полягає у побудові шляху від однієї вершини структури до довільної іншої вершини. Ця аномалія суперечить принципу зв'язності предметної області W_i.

Розглянемо наступне положення.

Положення 2.2. Предметна область інтерпретації деякої системи є завжди зв'язною на структурному рівні.

Структурна аномалія може мати місце у випадку, коли існує в структурі вершина, з якої не має виходу. Необхідність виходу з довільної точки пов'язується з відкритістю предметної області $W_i(IS)$. Логічна аномалія al в IS ілюструє той факт, що в рамках W_i існує логічна невідповідність між різними компонентами W_i. Введемо наступне положення.

Положення 2.3. Предметна область W_i не містить логічних суперечностей.

Оскільки логічна суперечність пов'язана з семантичною суперечністю відповідної області інтерпретації, на якісному рівні їх розділяти не будемо. Оскільки будь-який опис предметної області формується для розв'язання в рамках відповідної області певного класу задач, необхідно формувати її таким чином, щоб могли виникнути умови, що не дозволяють розв'язувати задані задачі недоцільно. Відповідні аномалії можуть виникати лише в тих випадках, коли W_i розширяється в процесі її використання.

Твердження 2.1. Якщо в IS існує система $R = \{r_1, \dots, r_m\}$ така, що $r_1 \prec r_2 \prec \dots \prec r_n$, то система R може бути розширена $r_{m+1} > r_m$.

Приймемо, що в SNP існує $R = \{r_1 \prec r_2 \prec \dots \prec r_m\}$. Обмежимося двома рівнями r_i і r_j. Це означає, що існує $r_i(x_i)$ і $r_j(x_j)$. Кожний рівень r_i і r_j визначається на основі використання критеріїв $k_1, \dots, k_m$. Оскільки r_i і r_j представляють собою деякі константи, а k_i представляє собою опис певних умов, що зв'язані з $r_i, \dots, r_m$, то в рамках W_i повинні існувати правила, за допомогою яких можна пов'язати k_i та r_i. Приймемо, що такими правилами є $P_1, P_2, \dots, P_k$. Оскільки існує $r_i(x_i)$, то це означає, що існує $j(x_i)$. Інтерпретація $j(x_i)$ виводиться з $J(W_i)$ у відповідності з системою залежностей $x_i = f(x_j, x_{j+1}, \dots, x_m)$. Оскільки всі $x_i \in W_i$ мають $j(x_i)$, то і всі $f_i(x_j, \dots, x_m)$ мають інтерпретацію $j[f_i(x_j, \dots, x_m)]$. Критерії k_i формуються в рамках W_i. Це означає, що правила $P_i[k_i, r_i, (x_j, \dots, x_m)]$ є виводимі в системі $\{\{k_1, \dots, k_m\}, \{r_1, \dots, r_k\}, W_i\}$. Приймемо, що в W_i реалізується деякий алгоритм $Al_i(x_i, x_j)$ такий, що $Al_i(x_i, x_j) \to x_i^*$. При цьому, $x_i^* \notin IS$. Оскільки кожний k_i визначає окремий діапазон значень на $R = \{r_1, \dots, r_m\}$ і $r_1 \prec r_2 \prec \dots \prec r_m$, то для x_i^* може існувати $j(x_i^*)$, яка приводить до виникнення суперечності в W_i. Для усунення відповідної суперечності, необхідно реалізувати розширення W_i. Оскільки x_i^* виникло в результаті виводу $Al_i(x_i, x_j) \to x_i^*$, то $x_i^* \in W_i$. Це означає, що $J(W_i) \to j(x_i^*)$. Критерії k_i представляють собою описи інтервалів, які розміщуються на відрізку їх визначення без розривів. Тому для розширення критеріїв є дві можливості. Це додавання відрізку перед k_1 і додавання відрізку після k_m. Розширення k_1 в сторону k_{i-1} не має сенсу, оскільки це приведе до того, що

$x_i^* \in \{x_{i1}, \ldots, x_{ir}\}$, для яких r_1 визначає вільний доступ до даних. Але такі x_i^* не можуть призвести до аномалії в W_i, оскільки вони є базовими для W_i. Тому необхідно проводити розширення k_m до k_{m+1}. Тоді k_{m+1} визначає рівень конфіденційності r_{n+1}, для якого виконуються співвідношення $r_{n+1} \succ r_n$. Оскільки $Al(x_i, x_j)$ не є суперечливим, то аномалія, до якої приводить x_i^* є семантична. Для усунення цієї аномалії використовується надання x_i^* нової категорії рівня конфіденційності r_{m+1}. Для побудови $j[r_{m+1}(x_i^*)]$ використовується висновок, що формується на основі використання наступних компонент:

– $j[Al_i(x_i, x_j)]$ – текстової інтерпретації алгоритму Al_i;

– $j[k_1, \ldots, k_m]$ – текстової інтерпретації критеріїв;

– $j(x_i)\&j(x_j)$ – текстової інтерпретації даних з IS, що формуються на основі $J[W_i(IS)]$.

Тоді можна записати наступне співвідношення:

$$\{j[Al_i(x_i, x_j)\&j(k_1, \ldots, k_m)\&J[W_i(IS)]]\} \to j[r_{m+1}(x_i^*)]$$

Рівень конфіденційності деяких даних залежить від кількості задач, які для свого розв'язання використовують дані відповідного рівня конфіденційності. Оскільки рівень конфіденційності $r(x_i)$ залежить від кількості користувачів, що звертаються до IS за відповідними даними, можна прийняти наступну інтерпретацію. Кожна окрема задача z_i приписується окремому користувачу h_i. У цьому випадку ми приходимо до ситуації, яка вже розглядалася і полягає у тому, що рівень конфіденційності знижується із збільшенням кількості користувачів, які використовують відповідну конфіденційну інформацію x_i.

Приймемо, що не існує можливості окремі задачі приписувати окремому користувачу. У цьому випадку результати розв'язання кожної окремої задачі використовуються в W_i. Кожне з таких використань розширює W_i, оскільки привносить нову інформацію в W_i, яка має свою власну інтерпретацію або $x_k = f(x_i, x_m)$ призводить до того, що $[j(x_k)\&j(f(x_i, x_m))] \to j(x_k)$, при цьому $j(x_k) \in J(W_i)$, а f_i визначає задачу z_i. При збільшенні кількості $z_i[r_m(x_k)]$, збільшується

кількість текстових описів $j(x_i)$ розширяють $J(W_i)$. Це означає, що між $(x^*_{k1}, \ldots, x^*_{km})$ та середовищем W_i з'являються додаткові зв'язки.

Кількість елементів з W_i збільшується, якщо на структурному та логічному рівні отримають зв'язок з $\{x^*_{i1}, \ldots, x^*_{im}\}$. Відповідно до прийнятої тези, рівень конфіденційності r_i залежить від кількості користувачів, які можуть звертатися за x^*_{ki}. Збільшення зв'язків між елементами еквівалентне збільшенню можливих задач, які можуть розглядатися у рамках певної системи.

Параметри, що визначають взаємозв'язки між даними, суттєво впливають на роботу SNP. Якщо дані x_i мають $r_i(x_i)$, а x_j мають $r_j(x_j)$ та $r_i \prec r_j$, то може виявитися, що користувач h_i використовуючи x_i, завдяки існуванню $x_j = \varphi(x_i)$, може несанкціоновано дістатися до x_j. Щоб цього не допустити SNP повинна перевіряти можливість реалізувати функції типу $\varphi(x_i)$ в оберненому напрямку. Це означає, що SNP повинна аналізувати близькість різних даних в IS. У даному випадку, віддаленість між різними елементами x_i і x_j з IS визначається рівнем складності переходу від одних даних до інших за рахунок зв'язку між ними. Якщо така віддаленість є недостатня для забезпечення заданої дисципліни розподілу даних по рівню r_i, необхідно вводити на відповідний зв'язок рівень конфіденційності r_i.

2.2 Аналіз функціональних можливостей та методу оцінки окремих компонент засобів захисту інформаційних систем

Інформаційна система, що орієнтована на надання послуг користувачам, має бути захищена від співпраці з несанкціонованими користувачами. Базовими компонентами захисту приймаються наступні:

- система захисту доступу до IS;
- система надання повноважень користувачам h_i;
- загальна система безпеки SB та інші.

У рамках даної роботи, в основному, будемо займатися системою надання повноважень *(SNP)* на використання та перетворення даних з різних компонент, що

входять в IS і може певною мірою захищати систему від несанкціонованих користувачів. Основною компонентною, яку захищає SNP, є база даних, за якими звертається користувач, а її елементами є дані x_i.

Для обґрунтованого захисту, необхідно визначати величину рівня такого захисту, який може визначатися рівнем конфіденційності груп даних. Це означає, необхідність розв'язання наступних задач в рамках системи SNP:

– визначити рівень конфіденційності $r_i(x_i)$;

– визначити класифікацію даних для об'єднання їх в групи;

– визначити необхідну кількість значень рівнів конфіденційності даних m.

Рівень конфіденційності даних $r_i(x_i)$ в процесі функціонування системи може змінюватися. Тому встановлення рівня конфіденційності повинно реалізуватися оперативно.

При цьому можуть мати місце ситуації, коли визначена оцінка необхідного рівня конфіденційності не відповідає рівням, що вже використовуються в системі. Тоді, необхідно додатково визначити, до якого найближчого рівня конфіденційності віднести отриману оцінку окремих даних. Оскільки рівень конфіденційності $r_i(x_i)$ і рівень значимості даних мають відмінні інтерпретації, то методи оцінки $r_i(x_i)$ та $\aleph_i(x_j)$ між собою повинні бути узгодженими. Рівень безпеки, який забезпечується для окремої IS, є інтегральним параметром, який об'єднує поряд з іншими характеристиками і рівень конфіденційності, як одну з оцінок, та рівень значимості окремих компонент системи.

Можливість класифікації даних обумовлюється наступними факторами:

– структурою системи, яка тісно пов'язана з її функціональними характеристиками та рядом інших вимог;

– задачами, що обумовлюються проблемами захисту і в першу чергу, використанням різних систем оцінок, що визначають необхідний рівень захисту;

– інтерпретацією інформаційного наповнення системи та інтерпретацією задач, що на її основі можуть розв'язуватися чи досліджуватися.

Визначення необхідних значень рівня конфіденційності даних чи компонент системи обумовлюється необхідністю забезпечувати безпеку не тільки функціонування самої системи типу IS, а і необхідністю забезпечувати безпеку предметної області, в якій розв'язуються задачі, що використовують ті чи інші дані системи IS. У цьому полягає суть використання поняття конфіденційності як оцінки певного рівня конфіденційності даних, що розміщаються в IS. Оскільки принципова різниця між оцінкою, що ґрунтується на величині рівня конфіденційності та іншими оцінками, що використовуються для визначення рівня безпеки, наприклад, величини ризику, полягає у тому, що оцінка рівня конфіденційності в основному пов'язана з величиною безпеки не самої IS, а безпеки предметної області, у якій розв'язується задача, що використовує конфіденційні дані, то необхідно більш детально розглянути задачу зв'язку системи IS з предметною областю W_i. Природно припустити, що будь-яка система типу IS чи просто інформаційна система, тісно пов'язана з предметною областю W_i, на яку IS орієнтована. Це означає, що в IS доцільно розміщати не тільки дані, які можуть бути потрібні користувачам для розв'язання тих чи інших задач, а й інформацію про користувачів та, в першу чергу, про предметну область W_i, яку IS повинно обслуговувати. Оскільки $r(x_i)$ пов'язана з небезпеками в середовищі W_i, то доцільно розширити інформацію про такі небезпеки. Для опису таких небезпек не достатньо даних з їх мінімальною інтерпретацією, яка забезпечується структурою даних, а необхідно IS розширити наступними даними та інформаційними елементами IS:

– значеннями даних, що відображають небезпечні ситуації в зовнішньому середовищі W_i;

– дані про користувачів, на яких у системі є інформація, що необхідна для розв'язання задач захисту доступу в систему IS;

– інформація та дані про можливі аномалії, що можуть виникати в W_i і суттєво впливати на зменшення величини рівня безпеки із зовнішнього середовища;

– інформація про окремі фрагменти реалізації різних способів перетворення та використання даних, що знаходяться у системі, які можуть або повинні використовуватися потенціальними користувачами системи IS.

У цьому випадку задача визначення необхідного значення рівня конфіденційності $r(x_i)$ для даних чи елементів x_i може розв'язуватися в рамках IS в автоматичному режимі без втручання власників відповідних даних у процес визначення величини $r_i(x_j)$, як це має місце в традиційних ситуаціях [76, 77]. Приймемо, що система SNP співпрацює тільки з санкціонованими користувачами, оскільки це повинна забезпечувати система доступу разом із засобами захисту доступу ($SD\&ZD$). Таким чином, визначення можливості надання чи не надання інформації певного рівня конфіденційності $r_j(x_i)$ санкціонованому користувачу, на рівні з іншими критеріями, визначається з урахуванням можливості псевдо передачі цих даних несанкціонованому користувачу (NK). Використання терміну псевдо передачі означає, що можуть існувати механізми, які дозолять користувачу типу NK отримати дані, що характеризуються рівнем конфіденційності $r_j(x_i)$, який є не допустимим для передачі відповідних даних NK. У цьому випадку необхідно розв'язати задачу, яка повинна встановити на основі яких можливостей SK може отримати доступ до даних заданого рівня конфіденційності. Щоб систематизувати можливі підходи до вирішення цієї задачі приймемо наступні визначення, якими будемо користуватися в даній роботі.

Визначення 2.4 Система доступу разом із засобами захисту доступу ($SD\&ZD$) розв'язує задачу визначення: чи користувач, що звернувся до IS, є санкціонований і ця задача розв'язується на основі аналізу даних, що характеризують самого користувача.

У відповідності з приведеним визначенням приймемо, що $SD\&ZD$ розв'язує задачу авторизації користувача, що можна описати наступним співвідношенням:

$$\left\{SD[k(p_1^k,\dots,p_r^k)]\&ZD(p_1^{SD},\dots,p_l^{SD}) \to Al^D\left(p_1^k,\dots,p_r^k,p_1^{/D},\dots,p_e^{lD}\right)\right\} \to$$

$$\to \{[(k \to sk)\&\neg(k \to NK)] \vee [(k \to NK)\&\neg(k \to sk)]\},$$

де p_i^k – параметр користувача, p_e^{lD} – параметр системи доступу, Al^D – алгоритм ідентифікації та авторизації користувача, що звернувся до IS із запитом по інформацію, k – користувач, статус якого є невизначеним в $SD\&ZD$.

Визначення 2.5. Система надання повноважень розв’язує проблему, що полягає у визначенні: чи задача, для розв'язання якої користувач SK звернувся до системи, має повноваження на використання відповідних даних, тобто чи використання задачею Za_i даних $r_j(x_i)$ не призведе до недопустимих ситуацій в середовищі W_i, на яке орієнтована відповідна задача.

Приведене визначення свідчить, що система SNP не стільки надає повноваження користувачу, скільки надає повноваження задачі на використання тих чи інших даних. Таким чином загальна система безпеки IS організує процес свого функціонування з наступними чинниками, що звертаються до системи:

– користувачем, якого ідентифікує і верифікує $(SD\&ZD)$ на основі даних і параметрів, які характеризують його, а система в результаті аналізу цих параметрів надає користувачу статус санкціонованого чи не санкціонованого або $SK \vee NK$;

– задачею, яку представляє SK системі і потребує тих чи інших даних для активізації свого процесу функціонування або процесу розв’язання.

Зі сторони IS система безпеки SB використовує систему надання повноважень SNP для надання повноважень на використання даних, що потрібні для розв’язання задачі, яку представив користувач.

Виходячи з цього можна стверджувати, що крім даних про користувачів, які використовуються системою $(SD\&ZD)$, засоби системи SB повинні володіти даними, які необхідні для встановлення повноважень деякої задачі Za чи встановлення відсутності повноважень у задачі Za_i використовувати дані, які відповідна задача потребує або визначення статусу задачі типу $N\ Za_i$. Формально цю ситуацію можна описати наступним співвідношенням:

$$\left\{\left[K\left(p_1^k,\dots,p_r^k\right)\&Za_i\left(p_1^z,\dots,p_g^z\right)\right]\rightarrow (SD\&ZD)\rightarrow Al^D\left(p_1^k,\dots,p_r^k,p_1^D,\dots,p_0^D\right)\right\}\rightarrow$$
$$\rightarrow\left\{Sk\left[Za\left(p_1^z,\dots,p_g^z\right)\right]\rightarrow (SNP)\rightarrow Al^{NP}\left(p_1^z,\dots,p_g^z,p_1^p,\dots,p_g^p\right)\right\}\rightarrow$$
$$\rightarrow\left\{Sk\left[Za\left[r_{j1}(x_1),\dots,r_{jm}(x_m)\right]\right]\rightarrow C\left[Za_i(y_{\mathrm{i}1},\dots,y_{ie})\right]\right\},$$

де p_i^z – параметри задачі, Al^{NP} – алгоритм визначення необхідних повноважень у задачі Za_i, p_i^p – параметри системи SNP, $r_{ij}(x_i)$ – дані x_i, що мають рівень

конфіденційності r_{ji}, y_i – результат розв'язання задачі, C – мета розв'язання задачі Za_i.

Для розв'язання таким чином сформульованої задачі забезпечення певного рівня безпеки системою $SB(IS)$ необхідно визначитися з параметрами задачі Za_i та з описом мети C_i розв'язання задачі $Za_i(y_{i1},\ldots,y_{ie})$. Дані, які знаходяться в IS, і особливо дані, що використовуються в прикладній задачі $Za_i(y_{i1},\ldots,y_{ie})$, не представляють собою деякі абстрактні величини. Вони завжди мають в рамках IS і, відповідно, в рамках W_i певну інтерпретацію, що записується у вигляді $j^s(x_i)$, якщо мова йде про інтерпретацію, що розміщається IS, та $j^W(x_i)$, якщо мова йде про інтерпретацію x_i в предметній області W_i. Прикладом інтерпретації x_i в IS є служити інформація про допустимий діапазон значень даних x_i. Практика побудови системи IS переважно не передбачає розміщення більш менш повної інтерпретації даних $j(x_i)$ в IS. Це призводить до того, що обґрунтування тієї чи іншої структури даних в IS залишається за межами IS у рамках процесів проектування системи. Це суттєво зменшує загальні можливості системи, особливо ті, що стосуються забезпечення заданого рівня безпеки даних, яку будемо позначати $\mu = f(SB)$. У рамках даного підходу дані, що розміщаються в IS, забезпечуються інтерпретаційними описами, повнота яких визначається рівнем конфіденційності r_i, рівнем значимості $\aleph_i$ та рівнем безпеки μ системи IS в цілому. Завдяки цьому проблема визначення необхідного рівня конфіденційності даних $r(x_i)$ може бути розв'язаною в рамках SNP, яка є функціональною компонентою всієї системи безпеки. По своїй суті опис інтерпретації $j(x_i)$ даних x_i відображає взаємозв'язки x_i з оточенням в W_i, рівень значимості x_i для W_i та рівень небезпеки, до якої може привести не коректний або не допустимий спосіб використання даних x_i в рамках W_i. Приймемо наступні положення, що відображають взаємозв'язок IS з предметною областю інтерпретації, до якої відносяться дані.

Положення 2.4. Будь-яка IS має власну W_i або власний фрагмент w_{ij} в загальній W_i.

Положення 2.5. Інтерпретація всіх даних x_i з IS $j(x_{is}),\ldots,j(x_{im})$ виводиться з опису інтерпретації W_i або $J(W_i) \to \forall j(x_i)[x_i \in IS]$.

Положення 2.6. Предметна область W_i представляє собою структурований опис всіх елементів $x_i \in W_i$ та всіх подій $y_i \in W_i$, які можуть виникати в W_i у результаті активізації процесів $f_i(x_{i1},\ldots,x_{im})$, що записується у вигляді співвідношення $y_i = f_i(x_{i1},\ldots,x_{im})$.

Для опису $y_i = f_i(x_{i1},\ldots,x_{im})$ використовуються системи правил, які залежать від способів опису W_i. Предметна область W_i може описуватися на різних рівнях загальності серед яких прийнято виділяти наступні [78, 79]:

– структурний рівень $S(W_i)$;
– логічний рівень $L(W_i)$;
– семантичний рівень $\sigma(W_i)$;
– розширений рівень опису $R(W_i)$;
– комбінований рівень опису $K(W_i)$.

Той чи інший рівень опису предметної області W_i і, відповідно, даних x_i використовується в залежності від задач, які передбачається розв’язувати, наприклад, структурний рівень опису $S(W_i)$ переважно використовується у випадках, коли задачі, що розв’язуються в рамках IS, представляють собою впровадження в IS та видачі з IS окремих даних. Якщо задачі, що розв’язуються в IS, орієнтовані на реалізацію перетворень даних з IS з метою отримання нових даних, необхідно використовувати логічний рівень опису предметної області [80].

Очевидно, що інтерпретаційні описи даних, які відносяться до W_i, повинні так чи інакше переноситися і в системи IS, які орієнтовані на обслуговування відповідної W_i. У кожній предметній області W_i можуть виникати негативні події, які визначаються на основі критеріїв, прийнятих в окремих W_i.

Такі негативні події можуть призводити до виникнення аномальних фрагментів або негативних ситуацій. Відображення таких негативних ситуацій у поточних описах фрагментів W_i залежить від рівня опису, який використовується.

Наприклад в описі, що реалізується на логічному рівні, негативні ситуації відображаються виникненням логічних аномалій [81].

При описі на семантичному рівні окремних фрагментів негативні ситуації відображаються у вигляді семантичних аномалій. Розширений рівень опису використовує не тільки текстові описи, а й інші форми відображення предметної області, наприклад, графічні фрагменти відображення різних аспектів, що мають місце в предметній області. Прикладом таких розширень можуть бути графічне відображення залежностей між змінними чи аналітичні описи залежностей і таке інше. Комбіновані методи відображення передбачають сумісне використання структурних і текстових форм відображення. Прикладом таких способів відображення можуть бути блок-схеми процесів, що відображаються у відповідних описах та інші. Введемо наступне визначення.

Визначення 2.6. Негативними факторами, що можуть виникати у W_i в результаті використання даних x_i з рівнем конфіденційності r_{ji} санкціонованим користувачем для розв'язання необґрунтованої задачі Za_i, є відповідні аномалії, що мають власну інтерпретацію.

У приведеному визначенні мова йде про санкціонованого користувача, яким є користувач, що пройшов ідентифікацію в системі ($SD\&ZD$). Це означає, що захищена IS системою доступу буде співпрацювати з користувачем SK. У рамках даного підходу довільний k_i звертається до IS не просто за отриманням тих чи інших даних, а у випадку, коли ці дані мають певний рівень r_i, тому k_i повинен надати системі обґрунтування необхідності їх використання для розв'язання конкретної задачі Za_i і ці обґрунтування представляють собою наступне:

– опис мети задач $C_i(K_i)$;
– параметри задачі $Za_i(P_{i1}^z, \ldots, P_{im}^z)$;
– обґрунтування необхідності розв'язання відповідної задачі.

Опис мети задачі по суті представляє собою опис фрагменту процесу функціонування, реалізація якого є однією із можливих складових всієї мети або $c_i(W_i) \in C[Za_i, W_i]$ та є обґрунтуванням необхідності використання даних типу $r_{ji}(x_i)$. Необхідність використання даних типу $r_{ji}(x_i)$ в Za_i підтверджуються

фрагментами алгоритму $Al_i(Za_i)$, що розв'язує задачу, яка приводить до досягнення мети і використовує дані $r_{ji}(x_i)$. Опис фрагмента $Al_i(Za_i)$ та $c_i(Za_i) \in C(Za)$ реалізується на рівні, який відповідає рівню, що використовується для розв'язання задач. Наприклад, якщо для опису використовується $L(W_i)$, то фрагмент алгоритму представляє собою відповідний фрагмент опису логічних перетворень з представленими даними серед яких є дані типу $r_{ji}(x_i)$. Оскільки система SNP на кінцевому етапі надає або не надає повноваження на використання $r_{ji}(x_i)$, то для цього достатньо визначити чи представлена користувачем SK ціль розв'язання задачі описує недопустиму в W_i ситуацію або подію. Якщо це має місце, то SNP не надає повноважень на використання $r_{ji}(x_i)$ користувачу SK при розв'язанні представленої користувачем задачі Za_i. Якщо ціль $C_i(Za_i)$ розпізнана, але не відома її інтерпретація, то SNP перевіряє представлені фрагменти $\varphi_i[Al_i(Za_i)]$ з метою визначення чи вони не приводять до виникнення логічної аномалії, прикладом якої може служити виникнення логічної суперечності в результаті здійснення відповідного перетворення.

Приведений опис може інтерпретуватися таким чином, що класифікація даних відповідно рівня їх конфіденційності у системі типу IS може в окремих випадках бути надмірною, оскільки щоразу, коли SK звертається за даними x_i, система SNP перевіряє чи їх використання в задачі Za_i не призводить до виникнення негативних ситуацій в W_i. У цьому випадку ситуація є досить складною і потребує початкового встановлення структури класифікації даних відповідно до параметру конфіденційності даних в силу наступних причин:

– процес визначення повноважень SK до використання в задачі Za_i даних $r_i(x_i)$ потребує певного часу та обчислювальних ресурсів і щоразу реалізувати цей процес по відношенню до даних, які, не можуть привести до аномалій в W_i, немає сенсу;

– при проектуванні IS на основі аналізу W_i встановлюється початкова необхідна кількість рівнів конфіденційності даних та формується структура організації цих даних і умови активізації SNP, які активізуються лише у випадку, коли SK звертається за певними даними типу $r_{ji}(x_i)$;

– проектування системи SNP потребує початкових даних для її реалізації основними з яких є: кількість рівнів конфіденційності $m(r_i)$, інтерпретація відповідних рівнів конфіденційності $j(x_i)$.

Важливим при такому підході є питання про формування шкали вимірювання рівня конфіденційності. Переважно така шкала будується на основі втрат, до яких приводить необґрунтоване, а тим більше, несанкціоноване використання $r_i(x_i)$. Такий підхід вносить певну суб'єктивність у відповідний рівень оцінки. Така суб'єктивність підсилюється у зв'язку з тим, що рівень конфіденційності з часом може зменшуватися через розвиток W_i та змінами, які в ній можуть відбуватися. Тому приймемо наступний підхід до динамічної корекції рівня конфіденційності окремих даних та до способу модифікації шкали конфіденційності. Така модифікація може полягати у зміні:

– величин масштабів рівня конфіденційності на окремих фрагментах шкал такого вимірювання;

– величин рівня конфіденційності на окремих рівнях, які були встановлені на етапі проектування;

– розмірів шкали вимірювання рівня конфіденційності.

Насамперед величини рівня конфіденційності тих чи інших даних будемо вимірювати не в коштах, що визначають величини втрат у випадку необґрунтованого використання $r_i(x_i)$, а у величині впливу відповідної аномалії на середовище, у якому вона виникла. Крім того, для визначення рівня впливу аномалій на W_i, будемо враховувати розміри аномалії, що може виникнути по відношенню до фрагментів, на які така аномалія впливає. Для кожного рівня загальності опису W_i шкали вимірювання величини впливу аномалії An_i будуть різні і рівень загальності опису An_i буде визначати рівень точності такого вимірювання. Оскільки шкала вимірювання величин конфіденційності формується на основі аналізу впливу аномалій на середовище W_i або $An_i \rightarrow W_i$, то відповідні величини визначаються на етапі проектування системи SNP. У процесі роботи SNP зміни масштабу вимірювання $r_i(x_i)$ здійснюються на основі даних про розміри аномалії, яка представлена в описі процесу розв'язання задачі та на основі визначення частоти

використання тих чи інших даних, що описуються параметром конфіденційності $r_i(x_i)$ і призвели до виникнення цих аномалій. Крім самого опису процесу реалізації відповідного фрагменту алгоритму, що використовує мету задачі (Za_i), система SNP використовує додаткові параметри, які характеризують $r_i(x_j)$. До таких параметрів відносяться наступні:

– інтервал часу використання $r_i(x_j)$ в процесі розв'язання (Za_i), який входить в інтервал часу реалізації всього процесу розв'язання Za_i;

– всі дані, що зберігаються в IS, мають окремі описи інтерпретації такого параметру, тому при використанні деякого параметру $r_i(x_j)$ в задачі Za_i такий параметр повинен мати величину рівня семантичної узгодженості, який в межах заданого діапазону відповідає величині, яка характеризує x_i в IS як окремий параметр даних типу $r_i(x_j)$;

– зв'язність даних типу $r_i(x_j)$ визначає кількість елементів з якими елемент $r_i(x_j)$ може взаємодіяти в процесі реалізації $Al_i(Za_i)$. При цьому враховується рівень конфіденційності таких елементів.

Ці параметри приписуються елементам $r_i(x_j)$ на стані проектування і використовуються: при визначенні рівня обґрунтованості, наданні цих даних, визначенні повноважень до їх використання відповідною задачею. Користувач SK, який активізує виконання задачі Za_i і потребує дані типу $r_i(x_j)$, повинен мати інформацію про ці параметри, які визначаються середовищем задачі, що розв'язується, і такі дані повинен надавати для обґрунтування необхідності отримання повноважень на активізацію задачі Za_i. Кожний фрагмент інформації, який будемо позначати символом $\Psi_i(x_j)$, представляє собою деяку числову величину, яка розширюється описом текстової інтерпретації, що формально описується наступним співвідношенням:

$$\Psi_i(x_j) = x_j \iota < \alpha_{i1} * \ldots * \mathrm{A}_{ik} *> I < \xi_{j1}, \ldots, \xi_{jm} >,$$

де $\Psi_i(x_j)$ – елемент інформації з IS, x_j – числова величина $\Psi_i(x_j)$, α_{ij} – фраза текстового опису інтерпретації $\Psi_i(x_j)$, яка пов'язує x_j з текстовими та іншими

описами предметної області W_i, ξ_{ij} – параметри x_j, про які йшла мова вище. Якщо має місце $r_i(x_j)$, то це означає, що рівень конфіденційності поширюється на весь інформаційний елемент $\Psi_i(x_j)$. Залежно від рівня конфіденційності r_i, відповідний фрагмент може використовуватися обмежене число раз. Така величина використовується для опису $r_i(x_j)$ і є невідома SK. Величина, яка є параметром $\xi_{ij}[r_i(x_j)]$ відіграє ключову роль при визначенні повноважень на використання $r_i(x_j)$.

2.3 Інформаційні особливості визначення оцінок параметрів в системі надання повноважень

Під час побудови систем надання повноважень (SNP) розв'язується задача надання повноважень не користувачеві, який отримав статус SK користувача системи захисту доступу до інформаційної системи IS, а надається повноваження задачі, що представляється SK і потребує тих чи інших даних, включаючи дані, що відносяться до категорії конфіденційних або характеризуються параметром $r_i(x_i)$, де r_i – рівень конфіденційності даних x_i [82, 83]. Положення, яке приймається, полягає у тому, що рівень конфіденційності визначається на наступних етапах: на першому етапі визначається на основі експертних оцінок, при проектуванні IS на наступних етапах він визначається на основі аналізу представлених даних про задачу, яка для свого розв'язання потребує дані, що характеризуються параметром конфіденційності r_i. На основі величини параметра r_i формується структура конфіденційних даних, яка має ієрархічний характер. У процесі функціонування системи IS рівні конфіденційності даних можуть змінюватися. Система SND для надання повноважень задачі Za_i на використання даних $\{r_i(x_j), \dots, r_m(x_{jk})\}$ аналізує наступні дані: параметри задачі та даних, за якими звертається задача, аналізує ціль, яку в результаті розв'язання задача передбачає досягти та аналізує обґрунтування необхідності розв'язання задачі [84]. Перші два фактори представляються зрозумілими на якісному рівні. Третій фактор потребує додаткового аналізу,

оскільки стосується обґрунтування необхідності розв'язання задачі, яке в традиційному розумінні цього терміну ніяк не пов'язувалося з процесами аналізу систем типу SNP чи $(SD\&ZD)$. Розглянемо наступні положення, які будемо вважати основою для проведення аналізу обґрунтованості розв'язання задачі Za_i, що співпрацює з SNP.

Положення 2.7. Довільна IS, що орієнтована на обслуговування предметної області W_i, містить усі дані про W_i, які необхідні для обслуговування запитів користувачів даних з W_i та для забезпечення всіх вимог за такого обслуговування, включаючи умову забезпечення захисту обслуговування.

Приведене положення означає, що IS повинна містити не тільки дані, що відображають поточний стан W_i, а і всю інформацію, необхідну для забезпечення параметрів обслуговування, узагальненням *яких будемо розглядати параметр*, що визначає необхідний рівень безпеки обслуговування. У цьому випадку система W_i в цілому і система SNP конкретно повинна мати необхідну інформацію для забезпечення заданого рівня безпеки. Тому розглянемо якого типу інформаційні особливості використовуються для визначення обґрунтованості потреби у розв'язанні поточної задачі Za_i на основі використання системи IS або на основі використання конфіденційних даних з IS, що використовує система SNP. До такого типу інформаційних особливостей відноситься використання не тільки даних, а й їх інтерпретацій, які формуються в рамках IS, і для використання такої особливості немає необхідності проводити додатковий аналіз системи IS. Цей аспект відображає виконання умови незалежності функціонування IS від W_i. До інших інформаційних особливостей відноситься наступні:

– якщо були звернення до IS за інформаційними елементами, у наданні яких IS відмовив через їх відсутність у системі, хоча ціль задачі передбачала їх використання в процесі розв'язання, то цей факт використовується як інформаційна особливість, що характеризує систему і задачу Za_i;

– інформаційною особливістю є ситуація, коли параметри поточної задачі Za_i відрізняються від параметрів попередніх задач Za_j на величину, більшу заданого

порогу δ^c, який визначається на основі аналізу цілей задач Za_i, Za_j, а також, якщо дані, що використовуються для її розв'язання відрізняються від даних інших задач не більше ніж на величину заданого порогу δ^D;

– інформаційною особливістю є ситуація, коли виконується попередня умова, але мета задач рівна в межах δ^c, а дані, що використовуються для розв'язання задачі, відрізняються від даних попередніх задач на величину, більшу ніж задана величина порогу δ^D.

Перший тип інформаційної особливості, що використовується як обґрунтування необхідності розв'язання задачі Za_i полягає у наступному. Оскільки IS, насамперед, орієнтована на надання даних користувачеві, то у випадку, коли система мусить відмовити у наданні послуги, задача, яка повинна надати IS додаткову інформацію, що орієнтована на елімінацію такої ситуації, в результаті чого задача може бути прийнята як обґрунтована. Це обґрунтування визначається на основі аналізу мети, в якій описується факт поповнення IS деяким класом даних з предметної області W_i.

Друге обґрунтування полягає у аналізі чи мета розв'язання задачі достатньо відрізняються для вибраного класу задач від мети попередніх задач. Ця умова є гарантією того, що різні користувачі не звертаються до IS за даними для розв'язання однієї і тієї ж задачі, які в заданому наближенні є однаковими. У цьому випадку IS може надавати додаткову послугу SK, яка полягає у тому, що IS надає інформацію відповідному користувачу про те, що задача, з якою звернувся SK до SNP, уже розв'язувалася. Якщо нова задача SK полягає у повторному запиті до одних і тих даних, цей факт реєструється в $SB(IS)$ і активізується перевірка актуальності повторного запиту за однаковими даними. У цьому випадку SB може перевіряти чи повторний раз звертається той самий SK чи інший та може виконувати інші додаткові перевірки, які визнаються заданим рівнем безпеки.

У третьому випадку аналізуються дані, які передбачаються використовувати для розв'язання задач. Якщо ці дані достатньо відрізняються від даних, що використовувались в інших задачах Za_i, що визначається порогом δ^D, а ціль

розв'язання задачі подібні в межах заданого порогу подібності δ^c, то така інформація враховується при визначенні обґрунтування необхідності розв'язання відповідної задачі.

Для якісної реалізації описаних умов надання повноважень системою SNP необхідно формалізувати відповідні процедури. Завдяки цьому виникає можливість їх узагальнити, довести несуперечність у рамках реалізації відповідного аналізу та довести інші властивості відповідних алгоритмів реалізації процесів надання доступу, наприклад їх повноту. Крім того формалізація опису відповідних процедур дозволить встановити додаткові залежності між елементами відповідних алгоритмів. Введемо наступні визначення і положення.

Визначення 2.7. Перетворення $F(x_{i1}, \dots, x_{ik})$, що реалізуються системою SNP, називаються замкнутими, якщо при реалізації $F(x_{i1}, \dots, x_{ik})$ використовується тільки ті x_{ij}, що знаходяться в $C_i(Za_i)$ та IS.

Положення 2.8. Процеси, що реалізуються в SNP повинні бути замкнутими, тобто реалізуватися у рамках IS.

Приведене положення орієнтоване на забезпечення автономії роботи SNP, що є одним з важливих факторів забезпечення безпеки. Мета розв'язання задачі може бути описана у вигляді логічної формули: $Za_i \rightarrow C_i(Za_i) = L_i^c(x_{i1}, \dots, x_{ik})$, де x_{ij} – змінні, що описують фрагмент $w_i \in W_{ij}$, який відповідає результату розв'язання, L_i^c – логічна функція, що описує $C_i(Za_i)$ на логічному рівні. Оскільки $C_i(Za_i)$ відноситься до W_i, а IS орієнтована на обслуговування W_i, то можна прийняти, що вся інформація, яку використовує $Al_i(Za_i)$, повинна бути так чи інакше представлена в IS. Коли йде мова про орієнтацію IS на W_i, це означає, що існує цілий ряд $IS_1, \dots IS_m$, які покривають всі аспекти, що стосуються W_i. Формально можна вважати, що IS є деяким узагальненням або об'єднанням всіх можливих $IS_1, \dots IS_m$. Розглянемо наступне твердження в рамках логічного опису W_i та IS.

Твердження 2.2. Якщо інформаційна система орієнтована на W_i, а задача Za_i обслуговує W_i з ціллю $C_i^t(Za_i)$, то в рамках засобів IS можна встановити наявність суперечності, яка може мати місце в $C_j\ (Za_i)$.

Якщо IS орієнтована на W_i, то ключові дані, що відображають W_i, знаходяться в IS. Множину таких даних будемо називати базовим універсумом W_i або $U(W_i)$.

Приймаємо, що ціль $C_i(Za_i)$ описується на логічному рівні наступним співвідношенням: $C^L(Za_i) = L_k^c[L_\lambda^c, \dots L_m^c]$, де L_i^c – фрагмент логічної формули $L_i^c = x_{1i} * \dots * x_{ik}$. Базовий універсум $U = \{x_i, \dots x_m\}$, де x_i – окремі дані IS, може бути розширений до U_i^*, де $U_i^* \in Al_i(Za_i)$, якщо для розширення використовується не суперечлива система виводу $\sum_i$. Для побудови процедури виводу $Al_i^* \in U_i^*$, критерії реалізації окремих кроків виводу формується на основі семантичного аналізу $j(x_i) \in IS$. Якщо маємо залежність $x_{i1} * x_{i2} *, \dots, * x_{ik} \to x_{j1} *, \dots, * x_{jm}$, то для вибору $\xi_{ij} \in \sum_i$ будемо використовувати критерії, що визначаються семантичними параметрами $\sigma[j(x_i)] * \sigma[j(x_j)] = P_i$, де $P_i \in [\alpha, \beta]$. Тоді критерієм буде величина $P_i \in [\gamma_{i1}, \gamma_{i2}]$, де має місце $[\gamma_{i1}, \gamma_{i2}] \subset [\alpha, \beta]$ з діаметром $\partial\gamma_i \le r_i$. Якщо має місце $\forall(x_i \in IS)[x_i \in W_i] \& \forall(x_j \in IS)[x_j \in W_i]$ та $x_i := j(x_i)$, $x_j := j(x_j)$, то в IS існує наступне $x_k := j(x_k)$, для якого маємо ще співвідношення:

$$[\sigma(x_k, x_i) \vee \sigma(x_k, x_j)] \in [\gamma_{i1}, \gamma_{i2}] \in [\alpha, \beta].$$

Розглянемо випадок, коли такий x_k в IS не існує. Тоді можна записати:

$$\forall(x_i \in W_i)\exists(x_k \in W_i)[\sigma(x_k, x_e) \in [\gamma_{i1}, \gamma_{i2}]].$$

Якщо це має місце і $\sum_i \in IS$ є не суперечлива, то існує вивід:

$$[(x_{i1} *, \dots, * x_{im}) \in IS] \to (x_{i1} *, \dots, * x_{im}) \to \exists x_e\{\sigma(x_k, x_e) \in [\gamma_{i1}, \gamma_{i2}]\}.$$

Таким чином існує наступний вивід:

$$\{\forall(x_{ij} \in IS)[(x_{i1} *, \dots, * x_{im})] \& \forall[x_{ik} \in C_i(Za_i)][x_{j1} *, \dots, * x_{jk}]\} \to \exists A_1(x_{ij} * x_{jk}) \& [\neg\exists A_2(x_{ij}, x_{jk}) = A_1].$$

Тому відсутність аномалії може бути доведена на основі використання:

$$[U \in IS] \& [C(Za_i)].$$

Важливою задачею, яка повинна розв’язуватися по відношенню до системи SNP, є задача визначення повноти цієї системи на алгоритмічному рівні [85, 86]. Це має наступну інтерпретацію в SNP. Система SNP при наданні повноважень повинна реалізувати алгоритми перевірок, які відповідали б вимогам системи безпеки SB. Це

означає, що кількість рівнів перевірок надання повноважень повинна відповідати кількості рівнів конфіденційності або:

$$\left[\sum_{i=1}^{n} r_i(x_j) = m\right] \& \left[\sum_{j=1}^{k} \left(Al_j^p(Za_i)\right) \leq m\right],$$

де m – кількість рівнів конфіденційності r_i, Al_j^p – алгоритм перевірок, який може реалізувати одну або кілька перевірок. Кількість таких рівнів тісно пов'язана з кількістю різних можливостей з надання доступу. Такі можливості пов'язані з різними способами використання інформації, до якої надається доступ. Прикладом таких способів використання інформації можуть служити:

– читання даних (R_i);
– запис даних у відповідний рівень конфіденційності (Wr_i);
– перетворення чи зміна значення даних (PD);
– усування даних (UD).

Для забезпечення можливості використання додаткових рівнів конфіденційності крім тих, що зв'язані з типами перетворень даних, які будемо позначати $r_i^p(x_j)$, введемо рівні конфіденційності, які будуть визначатися наступними факторами. У рамках IS можуть існувати дані, які з їх статусом або їх певними характеристиками взагалі не повинні надаватися ніяким користувачам, а їх використання повинно реалізовуватися в рамках системи SNP. Це означає, що задача користувача Za_i, що має ціль $C_i(Za_i)$, яка для реалізації алгоритму $Al_i(Za_i)$ потребує, поряд з іншими даними, дані $r_i^t(x_j)$, де r_i^t – означає клас конфіденційності вищого рівня ніж рівень конфіденційності, $r_i^p(x_j)$, де r_i^p – рівень конфіденційності даних, з якими можуть реалізовуватися приведені вище перетворення або, який надає повноваження на здійснення перетворень $\{R_i, Wr_i, PD_i, UD_i\}$, не може використовувати відповідні дані в рамках $Al_i(Za_i)$. Всі можливі та необхідні перетворення над змінними $r_i^t(x_j)$ повинні виконуватися в рамках системи SNP. Це означає, що задача Za_i, яка потребує $r_i^t(x_j)$ не отримає x_j, а отримає результат перетворень x_j, в яких можуть приймають участь дані нижчих рівнів

конфіденційності. Відповідні перетворення називаються закритими, а їх алгоритми будемо позначати Az_i. Тому SNP, крім алгоритмів аналізу обґрунтованості деякої задачі Za_i, повинна містити алгоритм типу $Az_i[r_i^t(x_j)]$.

Розглянемо особливості використання алгоритмів Az_i, які будемо зіставляти деякі внутрішні задачі Zv_i. На відміну від задач Za_i, алгоритми $Az_i(Zv_i)$ орієнтовані на виконання визначених перетворень. Такі перетворення формуються на основі аналізу характеристик даних $r_i^t(x_j)$ та на основі аналізу описів повної їх інтерпретації. Для даних, що відносяться до класу конфіденційності $r_i^t(x_j)$, існують різні рівні такої конфіденційності. Введемо наступні визначення.

Визначення 2.8. Першому рівню конфіденційності даних $r_i^t(x_j)$, які використовуються при наданні повноважень задачі, відповідають дані $r_i^t(x_j)$, для перетворення яких в SNP існують визначені алгоритми $\{Az_j \dots Az_k\}$, що використовуються в процесі розв'язання задачі Za_i, замість фрагменту алгоритм Al_i самої задачі, за умови, що Al_i має фрагмент, у якому сформовано необхідні умови для реалізації зазначеного фрагменту. Це означає, що Al_i орієнтований на використання даних типу $r_i^t(x_j)$ та описується ціль його реалізації. На основі цих даних SNP обирає адекватний $Az_i[r_i^t(x_j)]$ і передає результат перетворень до $Al_i(Za_i)$.

Формально це визначення можна описати наступним співвідношенням:

$$al_i[(x_{i1},\dots,r_i^t(x_i),\dots,)C_i(al_i)] \to NSPP$$

$$\{\forall(Az_i \in SNP)\exists Az_j[Az_j(x_{i1},\dots,r_i^t(x_j),\dots,x_{ik})] \to [C_i(Az_i) \approx C_i(al_i)]\} \to$$

$$\to \{[Az_i \to C_i(Az_i)] \to [C_i(Az_i \to Al_i(za_i))]\}.$$

Визначення 2.9. Другий рівень конфіденційності даних $r_i^{2t}(x_j)$, який використовується при наданні повноважень задачі, має місце у тому випадку, коли для досягнення цілі $C_i(al_i) \subset Al_i(za_i)$ в SNP не існує $Az_i(x_j)$, який забезпечував би досягнення цілі $C_i(Az_i) = C_i(al_i)$. На основі аналізу $C_i(al_i)$ та на основі аналізу інтерпретації $\{x_{j1},\dots,x_{jk}\}$ обирається алгоритм директивного характеру Az_i^d, який

формує результати обчислень, що зводяться до даних, які інтерпретуються на дискретній множині значень.

Основні етапи формального опису параметрів, що стосуються даних приведені на рисунку 2.1.

Етап 1. Прийняття рішень про надання повноважень:
$SNP \to C(Z_i)$; $h_i \to Z_i$; параметри Z_i; зовнішні засоби Z_i.
$p(z_i)=f\{r_i(Za_i), p[C(Za_i)], \aleph_i(Za_i), A[Z_i(W_i)], kr_i(x_1,\dots,x_n)\}$.

Етап 2. Аналіз суперечностей: An_i-? $\to$ W_iR -?

Етап 3. Аналіз можливостей розширення системи:
$R=\{r_1,\dots,r_m\}$ така, *що* $\{r_1 < r_2 < \dots < r_m\}$, то система R може бути розширена $r_{m+t} > r_m$.

Етап 4. Аналіз функціональних можливостей та методу оцінки окремих компонентів засобів захисту:
$\{SD[K(p_1^k,\dots,p_r^k)]\&ZD[p_1^{SD},\dots,p_l^{SD}] \to Al^D(p_1^k,\dots,p_r^k,p_1^{ID},\dots,p_e^{IO})\} \to 1 \to$
$\{[(K \to SK)\&(K \to \neg NK)] \vee [(K \to NK)\&\neg(K \to SK)]\};$
$\{[K(p_1^k,\dots,p_r^k)]\&Za_i[p_1^Z,\dots,p_l^Z] \to ZD \to Al^D(p_1^k,\dots,p_r^k,p_1^{ID},\dots,p_e^{ID})\} \to$
$\{SK[Za_i[p_1^Z,\dots,p_l^Z] \to SNP \to Al^{ND}(p_1^Z,\dots,p_r^Z,p_1^P,\dots,p_e^P)\} \to$
$\{SK[Za_i(r_{j1}(x_1),\dots,r_{jm}(x_m))] \to C[Za_i(y_{i1},\dots,y_{ie})]\}$.

Етап 5. Досліджуються інформаційні особливості визначення оцінок параметрів у системі надання повноважень: $al_i[(x_{j1},\dots,r_i^t(x_i),\dots,x_{jk})C_i(al_i)] \to SNP$
$\{\forall(Az_i \in SNP)\ \exists Az_j[Az_j(x_{i1},\dots,r_i^t(x_i),\dots,x_{jk})] \to [C_i(Za_i) \approx C_i(al_i)]\} \to$
$\to \{[Az_i \to C_i(Za_i)] \to [C_i(Az_i \to Al_i(Za_i))]\}$.

Рис. 2.1. Метод формального опису даних

На відміну від результатів використання даних $r_i^{1t}(x_j)$, які переставляють собою значення параметрів, що отримані з опису мети $C_i(al)$, при використанні алгоритму $Az_i[C_i(al_i)]$ дані, що отримані в результаті використання алгоритмів Az_i^d, представляють собою дискретну інформацію про необхідний варіант продовження відповідного алгоритму, якщо останній присутній Za_i або відповідні дискретні дані можуть означати наступне. Наприклад, якщо у випадку $r_i^{1t}(x_j)$, x_j – представляє собою величину, що допускає інтерпретацію значення з деякого діапазону значень, то дані, отримані в результаті використання $r_i^{2t}(x_j)$ і відповідно, алгоритму $Az_i^d[C_i(al)]$, представляють собою величини з бінарною інтерпретацією, яка визначає, наприклад, до якої області значень відноситься представлений результат.

Прикладом такої ситуації може бути інформація про те, що $x_i = Az_i^d\left[r_i^{2t}(x_j)\right]$ представляє собою величину, що є допустимою чи не допустимою для подальшого використання. В залежності від інтерпретації всієї Za_i і відповідних фрагментів W_i, інтерпретація отриманих даних $x_i = Az_i^d\left[r_i^{2t}(x_j)\right]$ може полягати у тому, що x_i має максимальне значення або мінімальне значення і т.д.

Алгоритми типу Az_i^d відносяться до класу дискретних алгоритмів, які використовуються для розв'язання задач на дискретних множинах даних [87, 88].

Визначення 2.10. Третій рівень конфіденційності $r_i^{3t}(x_j)$, який використовується при наданні повноважень задачі, має місце у тому випадку, коли на основі інтерпретаційних даних x_j та інтерпретації цілі $c(\mathrm{al}_i) \in Al_i(Za_i)$ приймаються рішення про неприпустимість безпосереднього використання x_j для розв'язання задачі Za_i, у зв'язку з чим система прийняття рішень (SPR), яка є складовою SNP, формує рекомендації щодо модифікації цілі $C(Za_i)$ в задачі Za_i з таким розрахунком, щоб можна було уникнути використання $r_i^{3t}(x_j)$.

Приведені визначення відображають тільки один фрагмент шкали рівня конфіденційності, який представляє собою розширення рівня, що відповідає в моделі Белла–Лападули рівню «цілком конфіденційно» [89], який називають класом конфіденційності. Прикладом усіх класів конфіденційності, що використовуються в цій моделі є:

– клас явної інформації (I);
– клас інформації обмеженого використання або клас інформації для службового використання (F);
– клас конфіденційної інформації (T);
– клас цілком конфіденційної інформації (S);

Відповідні класи при зростанні необхідного рівня захисту впорядковуються наступним чином: $I < F < T < S$. Якщо приведені визначення позначати узгодженими символами з символами, що використовуються в моделі Белла–Лападули [90], то рівень конфіденційності r_i^{1t} можна позначити $S1$, рівень конфіденційності r_i^{2t} – позначимо $S2$ і рівень конфіденційності r_i^{3t} позначимо $S3$.

Тоді приведене співвідношення для різних класів конфіденційності запишеться у наступному вигляді: $I < F < T < S < S1 < S2 < S3$. Очевидно, що розширення інших класів рівнів конфіденційності, таких як (F) і (T), є також можливим і потребує лише відповідної інтерпретації в рамках W_i і відповідно, в засобах захисту, що можуть використовуватися у тій чи іншій системі безпеки IS. Для формування загального підходу до побудови системи безпеки $SB(IS)$, розглянемо наступні положення, які визначають початкові умови, що повинні виконуватися.

Положення 2.9. Користувач, який використовує в Za_i початкові дані, повинен мати їх характеристику та ключові параметри.

Положення 2.10. Якщо $Al_i \in za_i$ використовує $r_i^t(x_j)$, то Al_i або його фрагмент $al_i \in Al_i$, що застосовує такі дані, повинен представляти собою опис причин та мети їх використання, який формально описується у вигляді:

$$(Al_i \in za_i) = al_{i1}\left[(x_{i1}^1,\ldots,x_{im}^1) *\ldots* al_{ij}^*\left[r_i^t(x_{j1},\ldots,x_{jk}), C_i(al_{ij}^*)\right]\right] *\ldots* al_{in}(x_{i1}^n,\ldots,x_{im}^n).$$

Визначення 2.11. Алгоритми $Az_i^d \in SNP$ описують декларовані перетворення даних з класів $r_i^t(x_j)$, які обираються на основі аналізу даних фрагмента al_{ij}^*. У разі, якщо такий вибір не забезпечує необхідної адекватності або величина $\left[\delta\left[(al_{ij}^*)\&Az_i\right] \le \delta z\right] \le \Delta\delta z$, обирається алгоритм перетворень Az_i^d, для якого результат перетворень відображається на дискретній множині, що може мати різну інтерпретацію.

Визначення 2.12. До складу SNP входить система прийняття рішень (SPR), яка розширює базовий перелік алгоритмів $Az_i \in SNP$ і підсумовує результат отриманого розв'язання до послідовності рекомендацій, які виводяться на підставі $al_{ij}^*[r_i^t(x_{j1},\ldots,x_{ik}), c_i(al_{ij}^*)]$ та відповідного алгоритму Az_i^d.

Розглянемо наступні ситуації, виникнення яких декларується приведеними визначеннями та положеннями. У залежності від величини збільшення конфіденційності в класі $S1$, відповідні дані користувачу можуть взагалі не надаватися, а необхідні перетворення в рамках дозволених операцій з останніми реалізуються в середовищі IS засобами SNP. Якщо рівень конфіденційності

інформації зростає до рівня $S2$, не тільки не надаються дані користувачу SK, а і результати їх використання надаються у певній формі, що суттєво знижує можливість розв'язати обернену задачу реалізації $al_{ij}^{*} \in Al_i \in Za_i$, що забезпечує високий рівень захисту даних. У випадку, коли рівень конфіденційності є $S3$, то алгоритм $Al_i(Za_i)$ отримує ряд певних рекомендацій щодо його реалізації в рамках Za_i і, відповідно, в рамках W_i, що робить неможливим формувати ті чи інші обернені реалізації можливих перетворень, щоб несанкціоновано отримати дані з рівня конфіденційності $S3$.

Приведені особливості реалізації системи SNP представляють собою опис можливих способів реалізації засобів захисту, що орієнтовані на забезпечення необхідного рівня конфіденційності типу $S1, S2, S3$. Очевидно, що в системі безпеки $SB(IS)$ повинні реалізовуватися також засоби безпеки, що орієнтовані на забезпечення рівнів конфіденційності F, T, S. Рівень забезпечення захисту I можна зіставляти з засобами безпеки доступу, на якому здійснюється ідентифікація і автентифікація користувачів.

У залежності від інтерпретації даних або інформаційних елементів IS і W_i можна розширювати рівні захисту в класах F, T, S, забезпечуючи таке розширення відповідними методами та засобами захисту, що реалізуються на основі класичних підходів до забезпечення безпеки системи IS [91, 92].

Оскільки SNP вирішує цілий ряд задач із захисту інформації рівнів $S, S1, S2, S3$, необхідно довести, що система правил, які реалізують відповідні засоби захисту є повна. У протилежному випадку могло б виявитися, що в рамках SNP можуть виникнути задачі, які не можуть бути розв'язані, що обумовлює некоректність функціонування SNP. Тому розглянемо наступне твердження.

Твердження 2.3. Система $\{SPR\&Az[r_i^{nt}(x_{i1}, \ldots, x_{ik})]\}$ в SNP є повна відносно $Al_i(Za_i)$, де $Za_i \in W_i$.

Основні етапи методу визначення параметру, що характеризують задачу, які відносяться до інформаційних запитів задач, приведені на рисунку 2.2.

Етап 1. На основі приведених вище визначень будуємо формальний опис алгоритмів в є Az_i (алгоритми, що знаходяться в SNP) при визначенні повноважень задачі:
$al_i[(x_{j1}, \dots, r_i^t(x_i), \dots, x_{jk})C_i(al_i)] \to SNP\{\forall(Az_i \in SNP)\ \exists Az_j[Az_j(x_{i1}, \dots, r_i^t(x_i), \dots, x_{jk})] \to [C_i(Za_i) \approx C_i(al_i)]\} \to \{[Az_i \to C_i(Za_i)] \to [C_i(Az_i \to Al_i(Za_i))]\}$.

Етап 2. На основі приведених визначень обираються алгоритми A_i^d формування директив, які використовуються на другому рівні конфіденційності при визначенні повноважень задачі.

Етап 3. На основі інтерпретаційних даних x_j та інтерпретації мети $C_i(al_i) \in Al_i(Za_i)$ приймаються рішення про недопустимість безпосереднього використання x_j для розв'язання задачі Za_i. Тому система прийняття рішень (SPR), яка є складовою SNP, формує рекомендації щодо модифікації мети $C_i(Za_i)$ в задачі Za_i і для того, щоб можна було уникнути використання $r_i^{2t}(x_i)$.

Етап 4. Аналіз суперечності окремої задачі.

Етап 5. Аналіз повноти $\{SPR\&Az_i[r_i^{nt}(x_{i1}, \dots, x_{ik})]\}$ в SNP є повна відносно $Al_i(Za_i)$, де $Za_i \in W_i$.

Рис. 2.2. Метод визначення параметрів прикладних задач

Це твердження означає що будь яка задача Za_i з W_i, яка використовує $r_i^{nt}(x_j)$ представленими засобами, буде мати розв'язання щонайменше у частині, що стосується змінних типу $r_i^{nt}(x_{j1}, \dots, x_{jm})$. Приймемо, що $Al_i^{/}(Za_i) = Al_i^{/}(x_{i1} * \dots * r^{nt}(x_{j1} * \dots * x_{jk})^i * \dots * x_{im})$. Тоді можна записати $Al_i^{/}(x_{i1} * \dots * r^{nt}(x_{j1}, \dots, x_{jk}) * \dots * x_{jm}) \to Al_i^{/}(x_{i1} * \dots * [r^{nt}(x_{j1}, \dots, x_{jk}), C_i(x_{j1} * \dots * x_{jk})] * \dots * x_{jm})$. Оскільки $Az_i(x_{j1} * \dots * x_{jk}) \to C_i(x_{j1} * \dots * x_{jk})$, то у разі, якщо довільна операція в $C_i(x_{j1} * \dots * x_{jm})$ недопустима за умов SNP, що відображаються в $Az_i(x_{j1} * \dots * x_{jm})$ у вигляді $Az_i(x_{j1} * \dots * (x_{ji} * x_{ji+1}) * \dots * x_{jk})$, то така операція буде замінена на операцію $\otimes$, яка у відповідності з Az_i є допустимою і тоді $Az_i(x_{j1} * \dots * (x_{ji} \otimes x_{ji+1}) * \dots * x_{jk}) \to C_i^*(x_{j1}, \dots, x_{jk})$. Якщо $Az_i(x_{j1} * \dots * \neg(x_{ji} * x_{ji+1}) * \dots * x_{jm})$, то це означає, що

$C_i(x_{j1} *\ldots* x_{jm}) \notin W_i$, неможливе, оскільки має місце $Az_i(x_{j1} *\ldots* x_{jk}) \rightarrow J\left(Az_i(x_{j1} *\ldots* x_{jk}) \subset J(W_i)\right)$ в силу побудови $Az_i \in SNP$. Покажемо, що в SNP існує така $\otimes$, що не призводить до $Az_i(x_{j1} *\ldots* \neg(x_{j1} \otimes x_{ji+1}) *\ldots* x_{jm})$. Якщо $(x_{ji} \otimes x_{ji+1})$ визначена в $J(Az_i)$, то для всіх операцій, що використовуються в $\sum_{i=1}^{n} Az_i$, використання $(x_{ji} \otimes x_{ji+1})$ має допустиму інтерпретацію, оскільки $J(W_i)$ є повна $aj(x_{ji} \otimes x_{ji+1}) \in J(W_i)$. Покажемо, що $C_i(x_{j1}, \ldots, x_{jm})$ при заміні $*\rightarrow\otimes$ не призведе ціль $C_i(x_{j1}, \ldots, x_{jm})$ до суперечності. Якщо фрагмент $(x_{ji} \otimes x_{ji+1})$ в $C_i(x_{j1}, \ldots, x_{jm})$ призводить до суперечності $\neg C_i(x_{j1}, \ldots, x_{jm})$, то $\{[C_i(x_{i1}, \ldots, x_{ik}) \backslash (x_{ji} \otimes x_{ji+1})] \rightarrow [C_i * \&(C_i^* \prec C_i)]\}$. Останній конюнкт означає, що ціль C_i^* зменшила область свого визначення або C_i^* звузила свої функціональні можливості, що елімінує можливість виникнення аномалії an_i. Це означає, що $Az_i \in SNP$ існує для довільного Al_i, оскільки $C_i(x_{j1}, \ldots, x_{ji-1}, x_{ji+1}, \ldots, x_{jk})$ може бути звуженим. Таке звуження може бути багатократним і може допровадити до того, що $c_i(x_{j1}, \ldots, x_{ik})$ елімінується з $Al_i(Za_i)$, що інтерпретується, як заборона розв'язання задачі Za_i використовувати $r_i^{nt}(x_{j1}, \ldots, x_{jk})$ в контексті $Al_i(Za_i)$.

Висновок до розділу 2

У другому розділі досліджуються методи визначення величини рівня конфіденційності, який змінюється у процесі функціонування IS. Проводиться аналіз особливостей рівня конфіденційності, який дозволяє виявляти фактори, що призводять до зміни цієї величини.

Уведено уявлення про параметр значимості даних та проводиться його аналіз. Вводиться ряд параметрів, що характеризують прикладну задачу.

У роботі запропоновано та досліджено особливості взаємозв'язку між процесами, що реалізуються в IS, та процесами, що функціонують в предметній області інтерпретації, яку обслуговує IS. У звязку з цим розглядаються різні рівні опису предметної області інтерпретації та їх використання у процесах захисту від негативних факторів, які можуть обумовлювати несанкціоноване використання даних з IS прикладними задачами.

Досліджуються процеси функціонування системи надання повноважень та доводиться твердження про можливість виявлення у рамках системи *IS* суперечностей у прикладній задачі, при звертанні останньої до *IS* за даними, що необхідні прикладній задачі для її розв’язання.

Вводиться та досліджується уявлення про три рівні конфіденційності даних та розроблено процеси управління системою надання повноважень при зверненні прикладної задачі до цієї системи за даними, що мають різні рівні конфіденційності.

РОЗДІЛ 3 Моделювання процесу функціонування динамічної системи надання доступу

3.1 Основні компоненти моделі захисту системи доступу

Модель динамічної системи захисту доступу (MZD) реалізує всі процеси, які передбачаються в системі, при розв'язанні поставленої задачі. До таких процесів відносяться наступні:

– ідентифікація і автентифікація користувачів $K_i(ID)$, задачі (Za_i);

– надання повноважень на використання даних задачі, яка звернулася за ними (SNP);

– управління рівнем конфіденційності даних $r_i\,(x_i\,)(URT)$;

– управління рівнем значимості даних $\aleph_i(x_i)(URZ)$;

– процеси оцінки $r_i\,(x_i\,)$, $\aleph_i\,(x_i\,)$ та параметрів інформаційних запитів задачі, що описується цими параметрами (OPS);

– процеси аналізу предметної області задач (APO);

– процеси визначення рівня безпеки системи типу IS по відношенню до небезпек доступу (ORB).

Ідентифікація та автентифікація користувачів відносно інформаційних систем типу IS має цілий ряд особливостей, які потребують додаткового аналізу [93]. Ці особливості обумовлюються специфікою інформаційних систем. До інформаційних систем, які мають власну специфіку, можна віднести системи соціального обслуговування громадян. Прикладом таких систем можуть бути системи медичного та податкового обслуговування. Системи IS, що мають власну специфіку, відрізаються від останніх наступними особливостями:

– інформаційні системи, орієнтовані на розв'язання певного типу задач, надають послуги лише особам, які мають певні повноваження до розв'язання відповідних задач;

– дані, що зберігають в IS, мають розвинену систему класифікацій відповідних даних;

– параметри, що характеризують дані, формуються на основі дослідження уявлень про небезпеки, які можуть існувати в галузі до якої відноситься окрема IS;

– преважна більшість даних використовуються лише для розв'язання задач, які стоять перед фахівцями відповідної предметної області інтерпретації;

– система захисту, яка забезпечує найнижчий рівень безпеки, є розподілена.

Виходячи з першої особливості, можна стверджувати, що системи типу IS не мають розподіленої системи доступу до конфіденційних даних.

Другою особливістю є те, що користувачі системи є підготовленими до роботи з нею, а також відповідні користувачі мають уже захищенні атрибути доступу, якими можуть бути спеціалізовані карти, орієнтовані на роботу з системою IS. Це означає, що система IS є більш захищена з точки зору доступності користувачів до системи. Засоби зовнішнього доступу до IS, які за своєю природою є більш захищеними, створюють додаткову зовнішню відносно IS систему захисту (ZSZ), яка керує та контролює процесами формування засобів доступу підвищеного рівня, керує процесами надання або призначення засобів доступу та аналізує інші функції, пов'язані з захистом доступу. У випадку системи ZSZ, у останньої існують широкі можливості з персоналізації засобів доступу. Ці можливості полягають у тому, що користувачі однозначно є досить класифіковані з точки зору їх прав та можливостей відносно IS.

Оскільки такі користувачі є фахівцями, а система IS орієнтована на розв'язання задач, то більшість з тих задач може бути визначена у рамках посадових обов'язків відповідних користувачів [94, 95].

Приймаючи до уваги описану вище особливість, можна сформулювати наступну задачу, що безпосередньо стосується системи доступу до IS в частині ідентифікації та автентифікації користувачів. Ця задача полягає у наступному. Приймемо, що на поточний момент часу t_i циклу функціонування IS, необхідно забезпечити рівень безпеки доступу (RBD) рівний деякій умовній величині ξ_i. У цьому випадку, необхідно визначити який рівень захисту доступу реалізувати в ZSZ

і яку частину рівня захисту реалізувати у системі захисту доступу, яка безпосередньо реалізується в рамках системи доступу, що є компонентою IS. Таку компоненту системи захисту доступу будемо називати внутрішньою системою захисту доступу (VSD). Отже загальна система доступу (ZSD) складається з двох компонент або має місце $ZSD = ZSZ\ U\ VSZ$.

Розподіл ZSD дозволяє використовувати наступні можливості:

– збільшити загальний рівень захищеності ZSD;

– розвантажити ресурси IS для її основних задач;

– підвищити ефективність рівня захисту доступу за рахунок того, що ZSZ більшою мірою може піддаватися зміні управляючими функціями;

– ефективно управляти дисципліною реалізації доступу користувачів до IS;

– використовувати суб'єктивні фактори для підвищення рівня безпеки доступу завдяки досить широкими можливостям управління користувачами, які є фахівцями відповідної установи.

Необхідність використовувати VSZ обумовлюється тим, що до системи IS повинні мати доступ окремі працівники, які не працюють в установі, що експлуатує IS. До таких працівників відносяться:

– фахівці, що працюють в установах, яким підпорядковується установа з IS;

– користувачі, які мають право доступу в особливих випадках чи спеціальних задачах, до розв'язання яких вони мають повноваження.

Ці випадки детально розглядати не будемо, але можливості використання VSZ передбачають їх врахування.

Більш того, у разі необхідності підвищення рівня безпеки IS, передбачатимемо можливість розширення контролю доступом власних фахівців, що є працівниками організації, яка експлуатує IS.

У цьому випадку користувачі K_i будуть проходити контроль доступу засобами ZSZ і VSZ.

Надання повноважень на використання даних, що відносяться до рівня конфіденційності $\mathrm{r}_i^z(x_i)$, надаються виключно задачам, які відповідні дані

потребують. Це означає, що користувач K_i, який готує задачу до розв'язання, повинен вводити до системи IS не просто запит на отримання даних, а описи їх інтерпретації $j(x_{i1}^z), \dots, j(x_{ik}^z)$. Індекс z у даних x_{ij} означає, що ці дані не можуть бути отримані користувачем на основі його повноважень. Очевидно, що $j(x_{ij})$ не можуть бути повними, оскільки в протилежному випадку такі дані були б відомі користувачу і не було б потреби перевіряти повноваження задачі Za_i. Дані з вибраними рівнями конфіденційності мають свій опис інтерпретації $j(x_i^z)$, що ці дані характеризують, які розділені в рамках структури параметрів, що їх характеризують. Описи інтерпретації $j(x_i^z)$ представляють собою деяку систему типу:

$$J(x_i^z) = F[j(x_{i1}^z * \dots * x_{ik}^z)],$$

де F – функція, що описує взаємозалежності між окремими $j(x_{ij}^z)$ та $j(x_{ie}^z)$.

Прикладом такої залежності може служити залежність між рівнями конфіденційності для цих складових, наприклад, може мати місце

$$[r_{ik}(x_{ij}^z) < r_{ig}(x_{ik}^z)] \& [\aleph_{ik}(x_{ij}^z) > \aleph_{ig}(x_{ik}^z)].$$

Це означає, що рівень $r_{ik}(x_{ij}^z)$ може бути доступним користувачу $K_i(Za_i)$, а рівень $r_{ig}(x_{ik}^z)$ є доступний лише для задачі Za_i. Надання повноважень певній задачі Za_i означає, що користувач K_i в умові задачі, яка вводиться в IS, описує для всіх вхідних даних $Za_i(x_{i1}^z, \dots, x_{ik}^z)$ всі відомі йому $j(x_i^z)$. Як уже зазначалося, K_i крім $x_{i1}^z, \dots, x_{ik}^z$ вводить до системи мету розв'язання задачі $C_i(Za_i)$, яка представляє собою деяке логічне наближення опису результату розв'язання Za_i. В $C_i(Za_i)$ описується результат у вигляді логічних залежностей між даними $y_{i1}, \dots, y_{ik}$. Таке наближення формується на основі інформації про мету розв'язання відповідної Za_i. Така мета, хоча б у наближенні, повинна бути відомою K_i, оскільки в протилежному випадку, опис задачі Za_i, який формує K_i, не є коректним. Виходячи з приведеного, можна стверджувати, що K_i готує опис вхідних даних $(x_{i1}, \dots, x_{ik})$ у вигляді опису їх інтерпретації $J[j(x_{i1}) * \dots * j(x_{ik}))]$, де кожний $j(x_{ij})$ є описом x_{ij} з наближенням, яке відповідає рівню поінформованості відповідного K_i. Для розв'язання задачі Za_i, яка представляється користувачем K_i, необхідна повна інформація про відповідні

дані. Тому система SNP на основі даних $Za[j(x_{i1}^z) * ... * j(x_{ik}^z)]$, визначає наступну інформацію:

– чи повноваження користувача K_i відповідають доступу до даних, що введені в задачу $Za[j(x_{i1}^z) * ... * j(x_{ik}^z)]$;

– на основі аналізу $j(x_{ij})$, SNP визначає їх рівень конфіденційності;

– використовуючи дані $C_i[Za_i[j(y_{i1}) * ... * j(y_{ik})]]$, система SNP встановлює наявність або відсутність суперечності в умові представленої задачі;

– оскільки IS, крім певних даних, має доступ до опису предметної області $W_i(DIS_i)$, на обслуговування якої орієнтована IS, то система SNP має можливість на основі даних про задачу Za_i отримувати додаткову інформацію про Za_i з $W_i(IS_i)$.

Перш ніж детально розглядати приведені аспекти функціонування SNP, введемо наступні визначення, які доповнюють систему IS в цілому.

Визначення 3.1. У рамках кожної IS_i визначаються критичні події, що можуть мати місце у відповідній області інтерпретації $W_i(IS_i)$, які будемо позначати символами $\mathcal{K}r_i(W_i)$.

Визначення 3.2. Кожна критична подія приводить до виникнення в W_i критичної ситуації $\mathcal{K}r_i(W_i)$.

Визначення 3.3. У предметній області W_i, на роботу з якою орієнтована система IS, критична ситуація виникає в результаті активізації відповідного процесу $Pr_{\text{і}}(\mathcal{K}r_i)$, який може виникнути у зв’язку з розв’язанням деякої задачі.

Визначення 3.4. Предметна область інтерпретації, що пов’язана з відповідною системою IS_i, має структуру $S(W_i)$, яка відображається на рівні логічних описів її фрагментів $g_i(\omega_i) \to L(\omega_i)$, а окремі фрагменти $\omega_i \in W_i$ складають графову структуру $G_i(W_i)$ предметної області W_i в цілому. Приведене визначення описується наступним формальним співвідношенням: $\{[g_{i1}(\omega_{i1}) \to L_{i1}(\omega_{i1})], \dots, [[g_{im}(\omega_{im}) \to L_{im}(\omega_{im})]\} \to GW_i$.

Розглянемо твердження про можливість виникнення суперечностей у процесі розв'язання задачі.

Твердження 3.1. Розв'язання задачі Za_i, в якій мета $C_i(Za)$ не суперечить умовам W_i, не призведе до виникнення елементу $\omega_i{}^*$, що обумовить виникнення суперечностей в $Pr_i(W_i^*)$, де $Pr_i(W_i^*) = Pr_i(W_i) * Pr_i(\omega_i^*)$.

Приймемо, що можна побудувати $G(W_j) \to \mathcal{L}_i(W_i)$, де $\mathcal{L}(W_i)$ певна сукупність $L_{ij}(\omega_{ij})$. Предметна область W_i формується відповідно до технічних умов, що описують W_i, які забезпечують розв'язання задач Za_i. Система IS є відображенням W_i у тій мірі, яка є необхідною, для розв'язання задач Za_i по відношенню до W_i. Це означає, що результат розв'язання ω_i^* задач Za_i з ціллю $C_i(Za_i)$, досягається процесом $P_r(Za_i)$, який використовує дані $Da(Za_i)$, які знаходяться в IS. Результат ω_i^* може представляти собою деякий фрагмент $S(\omega_i^*)$ структури $S(W_i^*) = S(W_i) \cup s(\omega_i^*)$ або певний елемент процесу $pr_i(w_i^*)$, який функціонує в рамках загального процесу, і описується як $pr_i(\omega_i^*)$.

Таким чином результат розв'язання задачі Za_i може приводити до події $V_i(\omega_i^*)$. Приведені інтерпретації результату розв'язання задачі Za_i в середовищі W_i, свідчать про створення фрагменту ω_i^*, виникнення процесу $pr_i(\omega_i^*)$ та про виникнення події $V_i(\omega_i^*)$ в W_i. Оскільки, загалом W_i допускає свою інтерпретацію у логічній формі $\mathcal{L}_i(W_i)$, то і ω_i^* можна інтерполювати логічною формулою $L_i(\omega_i^*)$.

Приймемо, що розв'язок задачі Za_i відповідає меті $C_i(Za_i)$. Система SNP, для прийняття рішення про надання Za_i даних $Da_i(Za_i)$, проводить перевірку мети $C_i(Za_i)$ на її зв'язок з початковими умовами Za_i та на її допустимість по відношенню до W_i. Допустимість $C_i(Za_i)$ визначається по мірі узгодженості даних, які потребує Za_i з даними в IS, що стосується відповідних фрагментів $\omega_i \in \mathrm{W}_i$. Коректність процесу $P_r(Za_i)$ ґрунтується на перевірці чи отриманий результат, що представлений у наближеній формулі опису мети, не буде суперечити логічній системі $\mathcal{L}(W_i)$. Оскільки $C_i(Za_i)$ може бути представлений у наближенні, яке представляє собою наближену логічну формулу $L_i[C_i(Za_i)]$, то існує можливість перевірки суперечності в рамках $\{\mathcal{L}(W_i)\&L_i[C_i(Za_i)]\}$. Оскільки таку перевірку здійснює SNP, то у випадку виявлення суперечності, SNP не надасть повноважень Za_i для отримання даних $Da(Za_i)$ з IS. Процес розв'язання задачі $Pr_i(Za_i)$

реалізується з допомогою алгоритму, який пов'язує сукупність $L(Za)\&L[C_i(Za)]$ з результатом розв'язання задачі, яким є ω_i^* або $pr_i(w_i^*)$. Якщо має місце співвідношення $\{L(Za_i)\&L[C_i(Za_i)]\} \to L(\omega_i^*)$, то це означає, що алгоритм $Al(Za_i)$ сформований коректно, по визначенню, оскільки у випадку, коли б мало місце $\{\mathcal{L}(Za_i)\&L[C_i(Za_i)]\} \to Al(Za_i) \to \urcorner L(\omega_i^*)$, то це означало б, що $\{L(Za_i)\&L[C_i(Za_i)]\}\&L[Al(Za_i)]\} \to (w_i)\&\urcorner(w_i^*)$ з чого виникало б, що $L(Za_i)\&Al(Za_i) \to \urcorner L(Za_i)$, що суперечить прийнятим умовам. Ця суперечність доводить, що має місце співвідношення:

$\{L(Za_i)\&L[C_i(Za_i)]\&[Al(Za_i)]\} \to [\mathcal{L}(W_i)\&\urcorner(w_i^*)]$.

Це означає, що $Al(Za_i)$ суперечна з $L(Za_i)\&L[C_i(Za_i)]$ або задача Za_i в цілому некоректна. Тому має місце $L(\omega_i^*)\&L(W_i) \to \mathcal{L}(W_i^*)$, що відповідає твердженню.

Наступним важливим параметром Za_i, який перевіряється системою SNP, є параметр значимості задачі $\aleph(Za_i)$. На відміну від значимості даних $\aleph_i(x_i)$, значимість задачі пов'язана з функціонуванням процесів, що активізуються в W_i. Значимість задачі, щоб підкреслити її відмінність від значимості даних, можна пов'язати з актуальністю задачі $Ak(Za_i)$. Однією з функцій SNP при формуванні рішення про надання тих чи інших даних задачі Za_i є визначення актуальності задачі $Ak(Za_i)$. Введемо її визначення.

Визначення 3.5. Актуальність задачі $Ak(Za_i)$ визначається рівнем прогресивності змін, які відбуваються в W_i, в результаті використання отриманого розв'язання задачі.

Для того щоб визначення $Ak(Za_i)$ було більш конструктивним, необхідно доповнити систему IS рядом критеріїв, що визначають прогресивність змін, при використанні в W_i результатів розв'язання задачі Za_i. У цілому IS можна розглядати, як ключовий засіб управління відповідною предметною областю W_i. Це обумовлюється наступними аргументами. Можна прийняти, що будь яка задача, яку передбачається розв'язувати, використовуючи дані з IS, орієнтована на активізацію або реалізацію прогресивних змін у середовищі W_i. Така теза є логічною, оскільки приймається, що управління W_i зі сторони відповідних установ, повинно

здійснюватися в позитивних цілях. Задачі Za_i, що використовуються, представляють собою фактори, що ініціюють процеси розв'язання задач, які допускають інтерпретацію, у відповідності з якою ці процеси можна розглядати як такі, що функціонують в W_i. У цьому випадку можна стверджувати, що коли процеси розв'язання задач активізуються на основі безпосередньої співпраці з IS незалежно від того чи та співпраця полягає в отриманні необхідних даних, чи сам процес реалізації розв'язання здійснюється в IS_i, результати такого розв'язання передаються в W_i і в останньому, на основі цього відбуваються зміни [96]. Вищезазначене свідчить, що в рамках IS, крім даних, що необхідні для розв'язання задач Za_i, повинні бути засоби, які б дозволили системі IS більш повно або більш широко приймати участь у процесі розв'язання задачі Za_i. Принципи, що закладаються в роботі, полягають у розподілі захисту доступу користувачів та функцій надання повноважень на використання тих чи інших даних окремим задачам, можуть бути розширені за рахунок перевірки рівня актуальності поточної задачі. Для цього в рамки SNP необхідно включити засоби визначення актуальності поточної задачі. Такі засоби можна реалізовувати різними способами, що відрізняються між собою складністю їх реалізації.

Найбільш простим способом реалізації необхідних засобів в SNP є спосіб, що полягає у наступному. Кожна задача Za_i для одержання повноважень повинна надати системі SNP опис мети розв'язання задачі $C_i(Za_i)$. Практично такий опис представляє собою інформацію про зміни в W_i, до яких призведе процес розв'язання Za_i. Оскільки W_i представляє собою опис деякого середовища, в рамках загальної системи управління таким середовищем декларуються критерії зміни значень параметрів в W_i, які визначаються позитивними. Відповідні декларації у формі, що пристосовані для їх використання в IS, розміщуються в системі. Тоді у найпростішому випадку, система SNP може здійснювати порівняння зміни значень параметрів, які введені до IS зі змінами цих значень, які пропонуються в описі мети задачі $C_i(Za_i)$. У даному випадку, не будемо розглядати конкретні механізми реалізації такого аналізу, оскільки його слід було б більш тісно пов'язувати з реальними прикладами предметної області та параметрами, що використовуються

для оцінки прогресивності змін у відповідному W_i. Для коректного відображення параметру $Ak(Za_i)$ введемо наступний його опис:

$$Ak(Za_i) = f[(P_{i1}^k, \dots, P_{im}^k), (P_1^{kr}, \dots, P_m^{kr})],$$

де f – може представляти собою, в найпростішому випадку, наступне співвідношення:

$$f[(P_{i1}^k, \dots, P_{im}^k), (P_1^{kz}, \dots, P_m^{kz}) = [\sum_{j=1}^{m}(P_{ij}^k - P_j^{kr})]/m,$$

де P_j^k – параметр, який відповідає параметру P_j^{kr}, але виконує роль критерія, який задається у системі SNP. Параметр P_{ij}^k – є відповідним до P_j^{kr} критерієм, який знаходиться в описі мети задачі Za_i або в $C_i[Za_i(P_{is}^k, \dots, P_{im}^k)]$.

Наступною важливою функцією моделі захисту даних MZD є оцінка рівня конфіденційності даних $r_i(x_i)$, які знаходяться в IS. Необхідність реалізації такої функції обумовлюється наступними причинами, до яких можна віднести:

– старіння параметрів даних;

– параметри, що характеризують процес використання конфіденційних даних;

– вплив змін значень інших параметрів, що безпосередньо зв’язані з параметрами конфіденційності;

– зміни умов функціонування в W_i;

– декларативні фактори.

Процес старіння рівня конфіденційності даних характерний для більшості параметрів, що характеризують об’єкти, у тому числі, й інформаційні. Це старіння полягає у тому, що дані, які довго зберігаються, через певний час уже можуть не відповідати дійсності, яка має місце в W_i, і тому поряд з іншими параметрами, значення параметра конфіденційності може з часом змінюватися.

Параметром використання даних може служити частота використання цих даних. Для W_i процеси натуральної зміни значення параметру конфіденційності даних є природним [97].

Вплив зміни значень параметрів, що безпосередньо зв’язані з параметрами конфіденційності, в рамках даної роботи, полягають у наступному. У рамках IS використовується характеристика важливості відповідних параметрів. Оскільки

значення цієї характеристики визначається в процесі функціонування IS і, відповідно, W_i, тому його значення може бути різним у різні моменти часу. Якщо приймати до уваги процеси старіння даних, оскільки цей фактор розглядається окремо, то можна стверджувати на якісному рівні, що параметр важливості $\aleph_i(x_i)$, зв'язаний з параметром конфіденційності. З точки зору загальних уявлень про параметр конфіденційності $r_i(x_i)$, останній є вищим, якщо він має більше значення для W_i. З іншого боку параметр важливості даних $\aleph_i(x_i)$ також допускає самостійну інтерпретацію його важливості для W_i. Розглянемо, у чому полягає різниця між ними на якісному рівні. Рівень конфіденційності даних x_i визначається, переважно, можливістю та величиною значень негативних факторів для W_i у випадку їх використання деякою задачею. Рівень важливості величини x_i або $\aleph_i(x_i)$ допускає інтерпретацію, яка полягає у тому, що ця величина визначається кількістю запитів за даними x_i або частотою їх використання при розв'язанні різних задач, орієнтованих на W_i. Ця різниця в інтерпретації визначила необхідність використання крім параметру $r_i(x_i)$, ще й параметр $\aleph_i(x_i)$. Оскільки в більшості задач Za_i окремо взяті параметри $r_i(x_i)$ чи $\aleph_i(x_i)$ не впливають автономно на кінцевий результат процесу $Pr(Za_i)$, то між ними, як і між іншими параметрами, що використовуються в $Al(Za_i)$ існує зв'язок, який визначається функцією $f_i(x_{i1}, \dots, x_{im})$, де $x_{i1} = r_i(x_i)$, а $x_{ik} = \aleph_k(x_k)$. Наприклад, достатньо часте використання параметра $\aleph_i(x_{ij})$ може призвести до збільшення негативної оцінки результату використання x_i. Це призводить до того, що одна і таж величина x_i може характеризуватися двома параметрами r_i та $\aleph_i$. Така ситуація є особливо характерною для окремих систем. Такий зв'язок або взаємний вплив між параметрами r_i та $\aleph_i$ особливо, коли вони відносяться до однієї величини x_i, є очевидним.

Випадки, коли має місце зміна умов функціонування W_i, що приводить до зміни значень параметрів $r_i(x_i)$ та $\aleph_j(x_j)$ є очевидними. Також очевидною зміною значень параметрів r_i та $\aleph_i$ є у випадку, коли ці зміни декларуються.

Основні етапи реалізації методу визначення компонент засобів захисту приведені на рисунку 3.1.

Етап 1. Система SNP на основі даних $Za[j(x_{i1}^z) * \cdots * j(x_{ik}^z)]$ визначає наступну інформацію: чи повноваження користувача K_i відповідають доступу до даних, що потрібні для вирішення задачі $Za[j(x_{i1}^z) * \cdots * j(x_{ik}^z)]$
Етап 2. На основі аналізу $j(x_{ij})$ SNP визначає рівень їх конфіденційності використовуючи дані $C_i[Za_i[j(y_{i1}) * \cdots * j(y_{ik})]]$, у зв'язку з цим система SNP визначає наявність або відсутність суперечності в умові представленої задачі.
Етап 3. Система SNP на підставі даних про задачу Za_i отримує додаткову інформацію про Za_i з $W_i(IS_i)$.
Етап 4. Аналіз критичних ситуацій.
Етап 5. Аналіз логічності структури $\{[g_{i1}(\omega_{i1}) \to L_{i1}(\omega_{i1})], \ldots, [[g_{im}(\omega_{im}) \to L_{im}(\omega_{im})]\} \to GW_i$.
Етап 6. Аналіз суперечностей.
Етап 7. Аналіз актуальності.
Етап 8. Аналіз значимості задачі.
Етап 9. Обчислення рівня безпеки *IS*.
Етап 10. Аналіз даних на базі рівня конфіденційності.

Рис. 3.1. Метод визначення компонентів засобів захисту

3.2 Обчислення рівня безпеки інформаційної системи

При проведенні аналізу процесу розв’язання деякої задачі з використанням інформаційної системи IS важливим параметром, що аналізується, є параметр безпеки, який стосується наступних компонентів:

– процесу розв’язання задачі;

– безпеки об’єкту на потреби якого розв’язується задача;

– безпеки даних, що використовуються для розв’язання задачі і знаходяться в IS чи вводяться в систему IS у результаті розв’язання задачі.

У залежності від самої інформаційної системи, що орієнтована на обслуговування деякого середовища W_i, загальний параметр системи може

складатися з цілого ряду окремих параметрів, що визначають загальний показник рівня безпеки β.

До таких складових входять:

– параметр конфіденційності даних ($r_i^t(x_i)$);

– параметр важливості даних $\aleph_i(x_i)$ або їх значимості;

– параметр актуальності задачі $Ak(Za_i)$;

– параметр безпеки задачі $\eta_i(Za_i)$;

– характеристика цілі задачі $C_i(Za_i)$;

– характеристика критичних ситуацій в W_i або $\mathcal{K}r(W_i)$;

– характеристика небезпек, що існують по відношенню до інформаційної системи IS або $Nb(IS)$.

Параметри та характеристики, що приведенні вище, безпосередньо впливають на величину безпеки системи та пов'язані між собою окремими залежностями. Крім того, ряд параметрів, виходячи з своєї природи, змінюються в процесі функціонування IS і, відповідно, залежно від часу і не залежно від подій, що пов'язані з порушенням безпеки системи зовнішніми факторами [98, 99].

Щодо параметру конфіденційності, то останній змінюється у часі, що називається процесом старіння конфіденційності $r_i(x_i)$ і це призводить до зниження рівня конфіденційності. Встановлено існування залежності між параметрами $r_i(x_i)$ та $\aleph_i(x_i)$. Параметр $\aleph_i(x_i)$ також підпадає під процес старіння, який приводить до його зменшення.

Параметр актуальності задачі $Ak(Za_i)$ з часом для окремих задач Za_i може зменшуватися, що також називається старінням задачі. Це явище обумовлюється тим, що $Ak(Za_i)$, як характеристика Za_i, залежить від параметрів даних, які задача використовує. Якщо параметри даних підлягають старінню, то і параметр $Ak(Za_i)$, який визначається поряд з іншими факторами та параметрами даних, також підлягає старінню.

Параметр безпеки задачі $\eta_i(Za_i)$ залежить не тільки від часу, протягом якого ця задача використовується, а і залежить від власних компонент, які цю задачу

складають. Першою з таких складових є мета розв'язання задачі $C_i(Za_i)$. Оскільки міра $C_i(Za_i)$ має власну характеристику $\varepsilon[C_i(Za_i)]$, то складові цих характеристик необхідно розглянути окремо.

Однією з ключових характеристик мети є її суперечність по відношенню до інших компонент задачі, до яких відносяться початкові умови або вхідні дані DW_i та алгоритм розв'язання задачі $Al(Za_i)$. Очевидно, щоб можна було цю характеристику визначити, відповідні складові мають бути представлені у вигляді своїх логічних наближень. Ця характеристика перевіряється системою SNP при розв'язанні задачі надання повноважень Za_i на використання даних.

Наступною характеристикою мети $C_i(Za_i)$ є її допустимість. Можливі критичні ситуації $\mathcal{K}r(W_i)$, що визначені в W_i, допускають інтерпретацію результатів функціонування задачі Za_i у середовищі W_i. Для довільного середовища W_i, на яке орієнтована система IS, характерними є фрагменти, які описуються як такі, що повинні виникати у відповідному середовищі. Очевидно можна було б стверджувати, що в описі W_i повинні представлятися тільки допустимі фрагменти, чи ситуації. Але таких фрагментів в результаті розв'язання задач може виникати достатньо багато. Заборонених ситуацій в W_i завжди є менше, ніж ситуацій дозволених. Тому для підвищення рівня безпеки W_i або $\beta(W_i)$ доцільно визначитися з усіма забороненими ситуаціями, які описуються у вигляді критичних ситуацій $\mathcal{K}r(W_i)$. Тому в рамках засобів захисту реалізується перевірка, яка формально описується співвідношенням:

$$\{C_i[Za_i(Dw_i)]\&Al_i(Za_i)\} \rightarrow \mathcal{K}r(W_i) \qquad (3.1).$$

Оскільки $Al(Za_i)$ орієнтована на досягнення мети розв'язання здачі, ця компонента використовується в рамках (3.1), і в цьому випадку враховуються всі чинники, що можуть призвести до виникнення $\mathcal{K}r(W_i)$. Ця характеристика $C_i(Za_i)$ визначається на бінарній множині, що означає:

– чи $C_i(Za_i)$ приводить до виникнення $\mathcal{K}r(W_i)$;
– чи не призводить до критичної ситуації.

Характеристика $C_i(Za_i) \rightarrow \mathcal{K}r(W_i)$ не завжди визначається достатньо однозначно. Справа у тому, що встановлені описи $\mathcal{K}r_i(W_i)$ на початковому етапі

формування W_i можуть у процесі функціонування системи $S[IS, W_i]$ змінюватися. У даному випадку мова йде про можливу зміну інтерпретації $\mathcal{K}r_i(W_i)$ або $J(\mathcal{K}r_i(W_i))$. Це є натуральним, оскільки в компонентах скредовища W_i заборони, що описуються $\mathcal{K}r_i(W_i)$, можуть змінюватися або, як мінімум, рівень критичності $\mathcal{K}r_i(W_i)$ може зменшуватися. Оскільки система IS є певним інформаційним відображенням відповідних W_i, то список всіх встановлених $\mathcal{K}r_i(W_i)$ повинен знаходитися в IS в підсистемі SNP. Загалом, у результаті функціонування IS до W_i можуть додаватися фрагменти, які можуть призвести до зниження рівня безпеки β за рахунок перетворення:

$$[J(\mathcal{K}r_i(W_i))\&J(IS)] \rightarrow J((\omega_1^*, \omega_2^* * \ldots * \omega_n^*) \rightarrow W_i r$$

Наступною характеристикою є рівень повноти опису мети розв'язання задачі. Насамперед, це означає, що у даному підході існує можливість з необхідним рівнем точності визначити можливий результат роботи Al_i на основі початкового опису задачі. З точки зору безпеки інформаційної системи, ця можливість є актуальною, оскільки в ситуації, коли розв'язання або результат розв'язання задачі недостатньо адекватний очікуваному, а система IS є базовою для забезпечення розв'язання задачі, то недостатня адекватність розв'язання задачі може інтерпретуватися, як недостатній рівень безпеки IS. Безпека самої системи IS не має сенсу, оскільки її безпека необхідна виключно для того, щоб при її використанні задачами не виявилося, що останні дають не адекватні або, взагалі не правдиві результати. Тому більш детально аналізувати задачі Za_i, які використовують дані з IS, не будемо, а обмежимося лише аспектами, які відносяться лише до IS. До параметрів інформаційного запиту задачі, які SNP перевіряє, для ідентифікації задачі, як окремого учасника, що співпрацює з IS, віднесемо наступні параметри:

– суперечність $C_i(Za_i)$ з початковими умовами $\sigma^i(C_i)$;
– актуальність задачі $Ak(Za)$;
– значимість задачі $\aleph_i(Za_i)$;
– рівень конфіденційності $r_i(Za_i)$.

Крім параметрів задачі у рамках SNP реалізується перевірка даних, за якими задача звертається до SNP. У зв'язку з цим задача Za_i повинна містити опис інтерпретації даних за якими вона звертається або $\{j(x_1^z), \dots, j(x_m^z)\}$. Такий опис повинен бути сумісним з описами відповідних даних, що знаходяться в IS, які можна записати у вигляді $\{j(x_1^D), \dots, j(x_m^D)\}$. Вибір відповідних даних реалізується на основі порівняння $\{j(x_i^z) = j(x_i^D)\}$. У межах IS частина $j(x_i^D)$ може представлятися елементами структури даних, а в межах Za_i весь опис $j(x_i^z)$ представляється у вигляді послідовної інформації, яка є зрозумілою для системи вводу запиту і системи пошуку відповідних даних. Для спрощення опису приймемо, що $j(x_i^D)$ і $j(x_i^z)$ представляють собою текстові описи на природній мові K_i, які ідентифікують дані x_i, що знаходяться в IS і, які формує K_i, при описі задачі Za_i або $j(x_i^z)$. Не будемо розглядати технічні деталі цих описів, які стосуються вимог щодо точності їх опису зі сторони K_i. Система SNP ідентифікує відповідні параметри моделі даних на підставі реалізації аналізу параметрів даних:

– аналізується рівень конфіденційності даних $r_i(x_i)$;

– рівень значимості даних $\aleph_i(x_i)$;

– рівень обґрунтованості використання даних у задачі Za_i, яка позначається $\lambda_i(x_i)$.

Приведені параметри, що використовуються в SNP для надання повноважень Za_i на використання даних $\{x_i^z, \dots, x_m^z\}$, можуть бути розширеними. Таке розширення реалізується на основі аналізу інтерпретації предметної області W_i або на основі $J(W_i)$. Очевидно, що IS, яка обслуговує W_i, повинна мати інтерпретацію, яка була б узгоджена з інтерпретацію $J_i(W_i)$, що описується наступним співвідношенням: $J(IS) \leftrightarrow J(W_i)$, де знак «↔» означає семантичну узгодженість між $J(IS)$ та $J(W_i)$. Така узгодженість може бути описана у вигляді:

$$\delta^u[J(IS), J(W_i)] = F(j(x_i^z), \dots, j(x_m^z), \dots, j(x_1^D), \dots, j(x_m^D)],$$

де F – функція, що описує рівень семантичної узгодженості [100].

Крім параметрів інформаційних запитів задачі, система SNP перевіряє характер інформаційних особливостей даних, що існують в рамках задачі. Для використання

цих параметрів у рамках моделі захисту доступу MZD система SNP формує профілі задач, які будемо позначати $\gamma(Za_i)$. Такий профіль відповідає певному періоду функціонування і після кожного етапу співпраці з Za_i відповідний профіль поповнюється або модифікується. По суті $\gamma(Za_i)$ представляє собою сукупність параметрів, значення яких змінюються в часі на інтервалі ΔT. Формально профіль $\gamma(Za_i)$ запишемо у вигляді наступного співвідношення:

$$\gamma(Za_i) = f[(P_1^I * P_2^I * ... * P_k^I), ..., (P_1^{Itk} * ... * P_k^{Itk}), \Delta t_i],$$

де f – функція, яка описує спосіб визначення інтегрального значення параметру P_k^{Itk} за період Δt_i, I – означає параметр інформаційного типу.

У більшості випадків функція f описує спосіб визначення середнього значення величини P_i^{Iti} на інтервалі Δt_i. До інформаційних параметрів P_i^I відносяться наступні:

– визначення, чи Za_i повинно поповнити IS новими даними з предметної області IS, (P_i^I – доповнення задачі);

– аналіз чи поточна задача Za_i не є повторенням задачі Za_i, яка уже розв'язувалась (P_p – повторення задачі), що визначається на основі співпадання мети цих задач;

– перевірка, чи поточна задача Za_i використовує ті самі вхідні дані, при різних цілях розв'язання задачі Za_i і однієї з попередніх задач Za_j (P_d – дублювання даних).

Кількість параметрів, які характеризують Za_i і використовуються при побудові профілю, можуть розширюватися, оскільки останні відображають предметну область W_i, на обслуговування якої орієнтована система IS [101].

Як уже зазначалося, параметри, що використовуються засобами захисту, складають деяку систему, яка має заданий рівень повноти. Введемо визначення, що стосуються загальної сукупності параметрів, завдяки чому можна визначати потрібну кількість параметрів, які необхідно використовувати для забезпечення того чи іншого рівня безпеки системи.

Визначення 3.6. Параметри моделей даних, параметри інформаційних запитів задач та параметри перевірки інформаційних особливостей задач складають систему параметрів, яка є повною для заданого рівня безпеки системи IS, що формально описується співвідношенням:

$$\beta(IS) = F[r_i(x_i), \aleph_i(x_i), \lambda_i(x_i), \delta^S(Za_i), Ak(Za_i), \aleph_i(Za_i), r_j(Za_i), P_c, P_d, P_p]$$

Рівень безпеки може визначатися на основі наступних підходів до його оцінки:

– на основі визначення можливих причин породження аномалій в W_i, що виникають або мають місце в IS, які будемо називати загрозами та позначатимемо Zg_i;

– на основі періодичного аналізу кількості аномалій в W_i та на основі аналізу негативних наслідків їх існування в W_i, не залежно від рівня безпеки системи IS або $\beta(IS)$;

– на основі аналізу зовнішніх факторів, які можуть виникати по відношенню до IS і приводити на кінцевому етапі до зниження рівня безпеки $\beta(IS)$.

Зовнішні фактори, які можуть виникати тільки в середовищі фахівців, що користуються системою IS, будемо називати атаками At_i. Тоді атаки реалізуються у вигляді звернень до IS, які представляють собою задачі, що потребують дані з системи. У зв'язку з тим, що користувачі K_i функціонують у рамках зовнішньої, по відношенню до IS системи безпеки, то приймемо, що причини пониження рівня безпеки $\beta(IS)$, що обумовлюються активізацією атак є достатньо мало ймовірні.

Підхід, що ґрунтується на основі періодичної перевірки аномалій, які виникли в W_i або критичних ситуацій, що мали місце в W_i, в результаті використання користувачами системи IS, переважно, проводиться в рамках аудиту поточного стану W_i і відповідно IS, яка реєструє виявленні відхилення, що виявляються на основі аналізу параметрів при наданні повноважень до використання даних. Аномалія $An(W_i)$, яка може існувати в W_i, відрізняється від критичної ситуації $Kr_i(W_i)$ тим, що $Al(W_i)$ може існувати деякий час в W_i і це приводити до погіршення параметрів функціонування W_i. Критична ситуація, яка може виникнути в W_i або в IS на відміну від $Al(W_i)$, може призвести до того, що в W_i чи IS

перестануть виконуватися окремі функціональні процеси, які є обов'язковою умовою того, щоб можна було говорити про той чи інший рівень безпеки функціонування W_i чи IS. Даний підхід до визначення $\beta(IS)$ чи $\beta(W_i)$ забезпечує визначення реального стану безпеки і носить констатуючий характер [102].

Більш конструктивним підходом до визначення рівня безпеки $\beta(IS)$ і, відповідно, $\beta(W_i)$ є підхід, що ґрунтується на аналізі сукупності параметрів, які перевіряються в SZD, з метою виявлення причин виникнення небезпечних ситуацій або подій в W_i і, в першу чергу, в IS. У цьому випадку необхідно встановити певні рівні безпеки на основі аналізу процесів функціонування IS. Оскільки IS разом з компонентами типу SB забезпечує, в першу чергу, безпеку для W_i, а засоби захисту реалізуються в IS, то приймемо, що будемо говорити про безпеку IS, яка природним чином поширюється і на W_i.

Розглянемо процес використання кожного з параметрів безпеки та проведемо аналіз можливих наслідків їх взлому або обходу по цих параметрах перевірок.

Насамперед розглянемо перевірки параметрів даних $r_i(x_i)$, $\aleph_i(x_i)$ та $\lambda_i(x_i)$.

За визначенням параметра $r_i(x_i)$, останній використовується для запобігання критичним ситуаціям $\mathcal{K}r(W_i)$. Як відмічалося, критична ситуація виникає в результаті події Vp_i, яка призводить до порушень в процесах функціонування W_i. Це означає, що ефект негативної дії, відповідної події Vp_i натупає відразу в W_i. Така ситуація, з точки зору безпеки, є найбільш несприятливою, оскільки в ній декларується настання негативних процесів. Основними причинами порушення контролю $r_i(x_i)$ є наступні. Задача Za_i для запиту даних, формує повідомлення, яке описує необхідні дані у вигляді деякого інтерпретаційного опису $j(x_i)$. При цьому Za_i може не мати інформацію про те, що відповідні x_i або $d(x_{i1}, \dots, x_{im})$ мають статус конфіденційних. За визначенням $j(x_i) \in Za_i$ не є повним, а представляє собою наближення до опису $j(x_i^*)$, яке є повним і знаходиться в IS. Це означає, що для опису $j(x_i)$ задача Za_i повинна виконувати певні вимоги з формування опису. Ці вимоги відповідають способам опису даних в IS. Приймемо, що $[x_i(IS) = j(x_i^*)] = Za_i * \dots * Za_j$. Тоді $X_i(Za_i) = j(x_i) =< a_i * \dots * a_k >$, де $k < m$, а a_i – окремі

інформаційні елементи, якими у випадку тексту є слова або фрази, а у випадку використання певних позначень ці елементи представляють собою відповідні коди або позначення.

При розпізнаванні x_i системою SNP остання приймає до уваги опис $j(x_i)$, який є коротким або який відрізняється від опису $j(x_i^*)$, що розмішений в IS. У цьому випадку задача розпізнавання в SNP запиту з Za_i величини $j(x_i)$ реалізується на основі аналізу $j(x_i) \in Za_i$ і $j(x_i) \in IS$. Оскільки $j(x_i)$ є не повним, то SNP повинна доповнити відповідний $j(x_i)$ і перевірити чи існує відповідна інформація в IS, яка відповідала б $j(x_i)$. Оскільки вимоги формування даних для Za_i і IS є однакові, то SNP реалізує доповнення опису $j(x_i)$ таким чином, щоб $j(x_i^*) * \xi(x_i) = j(x_i)$. Зрозуміло, що доповнення $\xi_i(x_i)$ до $j(x_i^*)$ можна здійснити різними способами, які залежать від:

- розмірів $j(x_i)$ та $j(x_i^*)$;
- вимог до способу побудови $j(x_i)$ в цілому;
- можливостей формування $j(x_i)$ в Za_i.

У даному випадку важливим є умова із забезпечення конфіденційності даних $r_i(x_i)$. Необхідність цієї умови ґрунтується на тому, що опис $j(x_i^*)$, який формується в Za_i, не повинен містити фрагменти інформації в $j(x_i)$, які стосувалися б даних, що обумовлюють їх конфіденційність певного рівня, оскільки Za_i не повинен знати рівня реальної конфіденційності даних $j(x_i)$.

Розглянемо наступне твердження.

Твердження 3.2. Система SNP забезпечує розпізнавання $r_i(x_i)$ за даними $j(x_i) \in Za_i$, якщо $j(x_i)$ збудовано відповідно до спільних для IS і W_i правил їх побудови.

Приймемо, що величина $r_i(x_i)$ є величиною дискретною. Це означає, що значення $r_i(x_i)$ можна індексувати. Тому для цієї системи $R = \{r_i, \dots, r_m\}$ можна записати структуру $r_1 < r_2 \dots < r_m$. Значення r_i для x_i вибираються на основі даних про $\mathcal{K}r_i(W_i)$, які розміщаються в IS. Приймемо, що $\mathcal{K}r_i(Vp_i)$, де Vp_i – подія, що обумовила виникнення $\mathcal{K}r_i(W_i)$, визначається на основі оцінки втрат на момент

формування опису W_i. Оскільки початковий варіант W_i є відомим, інакше не було сенсу будувати IS, то для проектних $\mathcal{K}r_i(W_i)$ можна визначити прямими підрахунками величини втрат $\{v_1, \dots, v_m\}$ для $\mathcal{K}r_1, \dots, \mathcal{K}r_m$, де $v_i = f(\mathcal{K}r_i)$ – функція визначення величини втрат. Тоді можна впорядкувати рівень конфіденційності $r_i \in R$. Приймемо, що кількість x_{ij}, для яких $r_i(x_i) = max\{v_1, \dots, v_m\}$, є найменша по відношенню до всіх можливих $r_j < r_i$. Це можна записати у вигляді $\sum_j^m Sg[r_{ij}] = m(r_i) < \forall\, r_j(r_j < r_i)$.

Таке припущення є обґрунтованим, оскільки через структурованість W_i всі $\mathcal{K}r_i(W_i)$ також структуризовані. Приймемо до уваги, що критичні ситуації пов'язані з рівнем конфіденційності даних. Це означає, що довільну $\mathcal{K}r_i(r_i)$ можна представити у вигляді наступного співвідношення:

$\mathcal{K}r_i(r_i) = F[\mathcal{K}r_1(r_1, \dots, r_{-1})]$, де $\mathcal{K}r_1 \& \mathcal{K}r_2 \& \dots \mathcal{K}r_{i-1} < \mathcal{K}r_i$.

Оскільки структура $\mathcal{K}r_i$ є більшою або складнішою від будь –якої $\mathcal{K}r_j$, де $j < i$, то $j(x_i) \to r_i$, повинен бути більшим від опису $f(x_{ij}) \to r_j$, якщо $r_i > r_j$. Оскільки Za_i зацікавлена в отриманні $r_i(x_i) \to j[r_i(x_i) > j(x_i)]$, то $j(x_i)$ формується таким чином, щоб $j(x_i)$ мала максимально можливий розмір у рамках правил та обмежень, що використовуються при складанні $j(x_i)$. Кожна задача формує описи $j(x_i^z)$ таким чином, щоб SNP могло розпізнати необхідну (x_i^D). Очевидно, що $j(x_i^z)$ не може містити повний опис x_i, бо тоді не було б сенсу використовувати r_i. Тому SNP реалізує вивід $[j(x_i^z) \& [j(x_1^D), \dots, j(x_m^D)]] \to r_i(x_i^z)$, що доводить твердження.

Одним з правил побудови $j(x_i)$ є правило, яке визначає мінімальну різницю у розмірах $j(x_i^z)$ для кожного x_i^z між описами x_i^z і x_j^z, які відносяться до суміщених рівнів конфіденційності. У зв'язку з цим, задачі Za_i і відповідно, користувачу K_i повинно бути відомими, до якого діапазону конфіденційності відносяться вхідні дані, за якими звертається задача Za_i. Ця вимога не мусить виконуватися для даних, які не мають параметру r_i.

Структура системи конфіденційності визначається наступним способом.

Визначення 3.7. Система R представляє собою лінійну дискретну структуру з неоднорідними кроками дискретизації або $R = \{r_1^{1t}, r_2^{2t}, \dots, r_M^{mt}\}$, де верхній індекс

означає номер рівня конфіденційності при заданому розподілі значень для кожного r_i.

У процесі функціонування IS структура R може змінюватися в силу природних змін в W_i та у зв'язку з процесами зміни значень параметрів, які є природними для систем типу IS. Очевидно, що такі зміни повинні реалізовуватися в рамках IS наступними процесами:

– в результаті процесів аналізу параметрів IS;

– в результаті впровадження нових даних в IS адміністраторами.

Параметр конфіденційності у рамках системи IS пов'язаний з іншими параметрами. Уже зазначалася, що r_i пов'язаний з $\aleph_i$ обернено пропорціональною залежністю, що виникає з інтерпретації r_i та $\aleph_i$.

Більш детально розглянемо зв'язок r_i з параметром $\lambda_i(x_i)$, який визначає обґрунтованість використання даних x_i в рамках алгоритму $Al_i(Za_i)$. Цей параметр не визначається факторами, що пов'язані з необхідністю використання деяких даних у відповідному алгоритмі. Розглянемо визначення.

Визначення 3.8. Обґрунтованість $\lambda_i(x_i)$ використання даних x_i в задачі Za_i визначається величиною різниці між цілями, одна з яких описує результат розв'язання задачі Za_i з використанням x_i, а друга –результат розв'язання тієї ж задачі без використання змінності x_i, що формально описується співвідношенням:

$$\lambda_i(x_i) = f\{C_i[Za_i)(x_1, \dots, x_i, \dots, x_m)] * C_i[Za_i)(x_1, \dots, x_{i-1}, \dots, x_{i+1}, .., x_i),$$

де f – функція, що описує спосіб обчислення різниці між цілями задачі – Za_i.

3.3 Модель багаторівневої системи доступу

Багаторівневі системи доступу до інформаційних засобів забезпечують можливість реалізації оптимальних процедур здійснення доступу до даних та інших засобів інформаційної системи. Кількість рівнів, що реалізуються у системі SNP, може визначатися наступними способами, пов'язаними з захистом даних.

На початковій стадії підготовки до запиту на доступ до даних, користувач, який ініціює відповідний запит має власні ідентифікаційні дані та інші дані, які потрібні для отримання доступу користувача K_i. Відповідний користувач K_i повинен сформувати дані про задачу, яку йому необхідно розв'язати, використовуючи дані з системи IS. Якщо користувач для розв'язання задачі не потребує конфіденційних даних певного рівня, він може звертатися до системи IS за отриманням цих даних. При цьому сама задача може розв'язуватися засобами, що не належать IS. Такий рівень доступу називається нульовим рівнем.

Перший рівень доступу полягає у наступному. Користувач K_i, що представляє задачу Za_i, яка потребує для розв'язання дані, що характеризуються рівнем конфіденційності, наприклад, першого рівня $r_i^{1t}(x_i)$, реєструється в системі доступу, а задача реєструється в системі наданням повноважень. Якщо система доступу автентифікувала користувача, то, у випадку, коли задача, для розв'язання якої потрібні дані, що мають перший рівень конфіденційності $r_i^{1t}(x_i)$, повинна системі SNP надати певні дані про задачу Za_i. Такі дані можуть мати різний склад, залежно від рівня конфіденційності даних, за якими звертається задача Za_i. Користувач вводить у систему задачу Za_i і може не знати, який рівень конфіденційності мають дані, що потрібні для задачі. Тому інформація про задачу повинна вводитися у повному обсязі. Після надання задачі повноважень фрагменти алгоритмів SNP, що стосуються використання $r_i^{1t}(x_i)$, реалізуються з допомогою алгоритмів, що знаходяться в рамках SNP і тільки результат цих перетворень, який уже не має рівня конфіденційності $r_i^{1t}(x_i^*)$, передається задачі і задача активізується з місця, для якого дані з SNP є вхідними. У зв'язку з цим виникають наступні задачі:

– введення алгоритмів, які можуть використовуватися для перетворень $r_i^{1t}(x_i)$ і включення їх до складу системи SNP, які позначаються Az_i;

– визначення, чи в результаті роботи $Az_i[r_i^{1t}(x_i)]$ отримані вихідні дані повинні не характеризуватися параметрами конфіденційності $r_i(x_i)$;

– перевірка, чи множина алгоритмів Az_i є повна з точки зору потреб, які можуть виникнути у окремих задач, що звернулися за даними $r_i^{1t}(x_i)$ до SNP.

Перша задача розв'язується на основі використання наступних положень.

Положення 3.1. Необхідність введення параметру конфіденційності для x_i^* обумовлюється наявністю можливого варіанту використання цих даних, який може призвести до виникнення критичних ситуацій $\mathcal{K}r_i$ у середовищі використання результатів розв'язання задачі яким є W_i.

Це означає, що не можна допускати можливість використання x_i^*, в результаті якого виникає $\mathcal{K}r_i$, що має негативну інтерпретацію в W_i. У зв'язку з цим необхідно довести, що всі можливі негативні ситуації $\mathcal{K}r_i(W_i)$, які на даному етапі будемо зіставляти з аномаліями An_i, складають обмежену множину і можуть бути визначеними в рамках W_i. Крім того, необхідно довести, що множина $\{An_i\}$ є обмежена і кожний елемент цієї множини на початковому етапі формування IS та W_i може бути визначеним.

Положення 3.2. Системи IS орієнтовано на обслуговування різних об'єктів, якщо вони потребують використання IS.

Розглянемо наступне твердження.

Твердження 3.3. Множина $\mathcal{K}r_i$ та відповідно множина An_i є обмеженими.

Будь-яка область інтерпретації W_i може бути представлена як деяка сукупність простих об'єктів $\{x_1, \dots, x_n\}$ та сукупність окремих процесів, що позначаються $\{Pr_i(x_{i1}, \dots, x_{im}), \dots, Pr_i(x_{j1}, \dots, x_{jn})\}$, які можуть взаємодіяти між собою. Така взаємодія реалізується в рамках загальних алгоритмів $\{Al_i, \dots, Al_n\}$. Для W_i характерно, що одні і ті ж $Pr_i(x_{i1}, \dots, x_u)$ не можуть одночасно використовуватися в різних $Al_i(Pr_i, \dots, Pr_m)$.

Приймемо, що для Al_i кожне Al_j відрізняється від Al_i кількістю різних процесів, які використовуються у відповідних алгоритмах. З іншого боку, кількість критичних ситуацій, що можуть виникнути в W_i в результаті Al_i, не більша кількості різних класів даних, що характеризуються параметрами конфіденційності r_i^{et}. Кількість даних типу $r_i^{et} \geq \mathcal{K}r_i(W_i)$. Протягом одного циклу функціонування IS, який рівний ΔT кількість $\mathcal{K}r_i$, буде визначатися співвідношенням $[(\mathcal{K}r_i, < r_i^{et}) \& (\mathcal{K}r_i, \leq$

$(Al_i(\Delta T))]$. Це свідчить, що на інтервалі ΔT кількість $\mathcal{K}r_i$ і, відповідно, An_i, які можуть виникати, є обмежена.

Оскільки наявність в IS даних $r_i^z(x_i)$ з часом може зменшуватися, то кількість $\mathcal{K}r_i$ з часом також буде зменшуватися. Введення нових даних типу $r_i(x_i)$ може реалізовуватися лише при розширенні W_i додатковими елементами $w_{ij} \in W_i$ або за рахунок ускладнення структури W_i, що записується у вигляді: $S_i(W_i) \to S_{i+I}(W_i)$.

Будь-які дані можна представляти певним чином адекватно їх інтерпретації. Це означає, що дані, які характеризуються параметром конфіденційності, також можна представляти або описувати з різним рівнем їх точності. Одна з характеристик даних $d_i(x_{i1}, \dots, x_{ik})$ представляє собою точність цих даних по відношенню до факторів, які вони відображають. Формально це можна описати наступним способом у вигляді співвідношення:

$$r_i^{et}(x_i) \to [j(x_i) = [j(\xi_{i1}) * \dots * j(\xi_{ik})]]] \to [j(\xi_{i1}) * \dots * j(x_{ig})]\&(g < k)\} \to$$
$$\{[r_i^{mt}(x_i^*) < r_i^{et}(x_i)]\&[x_i^* = [j(\xi_{i1}) * \dots * j(x_{ig})]]\}.$$

Це означає, що існує таке перетворення $r_i^{et}(x_i)$, яке може призвести до $x_i \to x_i^*$, де $r_i(x_i) > r_i(x_i^*)$. Таким перетворенням може служити алгоритм типу $Al_i(IS)$, який не є доступний користувачу K_i.

Якщо приведений вище процес модифікації інтерпретаційного опису величини x_i з метою зменшення рівня адекватності цього опису, що може відображатися зменшенням рівня точності x_i продовжити, то можна перейти до такого рівня адекватності опису, при якому x_i^* не зможе бути використаним для формування An_i в W_{ij}. А це означає, що x_i^* втрачає параметр конфіденційності $r_i(x_i)$.

У рамках даної роботи використання $r_i^{et}(x_i)$ для розв'язання задачі Za_i з цілю $C_i(Za_i)$, є можливим, якщо виконуються наступні умови:

$$[C_i(Za_i) \neq An_i(W_i)]V[C_i(Za_i) \to \urcorner An_i(W_i)] \qquad (3.2);$$

$$Za_i(x_{i1}, \dots, r_{ij}^t(x_{ij}), \dots, x_n) \to [(Za_i) \neq An_i(W_i)] \qquad (3.3).$$

У першій умові мова йде про те, що $C_i(Za_i)$ не представляє собою аномалію або з $C_i(Za_i)$ не може бути виведена аномалія. Друга умова відповідає випадку, коли

розв'язання задачі Za_i, яка використовує $r_i(x_i)$, приводить до мети $C_i(Za_i)$, що не представляє собою аномалій $An_i(W_i)$.

Для забезпечення приведених вище умов необхідно таким чином організувати роботу Al_i з даними, що мають рівні конфіденційності $r_i^{et}(x_i)$, щоб процеси перетворення цих даних були неможливими для довільних $Al_i \in Za_i$. Оскільки IS володіє не тільки даними типу $r_i^{et}(x_i)$, а і їх інтерпретаціями $j(r_i^{et}(x_i))$, а також даними про всі можливі $\mathcal{K}r_i(W_i)$, то в рамках IS можуть реалізовуватися фрагменти $Az_i \in Al_i$, які безпосередньо реалізують такі перетворення даних типу $r_i^{et}(x_i)$, які не призведуть до виникнення $\mathcal{K}r_i(W_i)$.

Твердження 3.4. Система $\{Az_i[r_i(x_i)], \dots, Az_m[r_m(x_m)]\}$ є повною відносно задачі Za_i.

Щоб довести твердження необхідно показати, що для довільної Za_i існує Az_i, яка забезпечує коректне використання будь-яких $r_i^{et}(x_i)$.

Система SNP перевіряє умову чи $C_i(Za) \to \mathcal{K}r_i(W_i)$, що реалізується на основі відомих описів $\mathcal{K}r_i(W_i)$ і представлених в Za цілей $C_i(Za_i)$. Крім того, SNP перевіряє чи $C_i(Za) \neq \mathcal{K}r_i(W_i)$, що також можливе, оскільки всі $\mathcal{K}r_i(W_i)$ є відомими системі IS. Якщо $C_i(Za_i) \to An_i(W_i)$, то Za отримує модифіковані дані $r_i^{et}(x_i) \to r_i^{gt}(x_i)$, де $g < e$ і проводить перевірку умови:

$Za_i[x_{is}, \dots, x_{in}, \dots, r_i^{gt}(x_i)] \to \{[C_i(Za_i)] \to [An_i(W_i)]\}$, якщо умова не виконується, то реалізується перетворення $r_i^{gt}(x_i) \to [r_i^{ht}(x_i^*)\&(h < g)]$ і проводиться перевірка умови (3.2). Якщо ця умова не виконується, то відповідне перетворення повторюється з елементом $r_i^{ht}(x_i^*)$ до того часу, поки умова (3.2) не стане виконуватися або поки $r_i^{kt}(x_i^*) \to r_i^{ht}\left(x_i^{n+1}\right)$, де – x_i^{n+1} перестає відноситися до конфіденційних даних. Оскільки алгоритми $Az_i[r_i^{it}(x_i)]$ є алгоритмами, що реалізують фрагмент перетворення Al_i з Za_i, то перетворення типу (3.3) виконується, а система $\{Az_i[r_i(x_i)], \dots, Az_i[r_m(x_m)]\}$ є повна.

З приведеного твердження виходить, що система IS, в цілому, і SNP не відмовляє задачі Za_i у наданні необхідних даних, а лише не допускає можливості окремій задачі Za_i, використовуючи конфіденційні дані, створювати у предметній

області W_i, що інтерпретує IS, не допустимі або критичні ситуації [103, 104]. Слід відмітити, що у наведеному випадку мова йде про вибраний діапазон рівня конфіденційності, який має певну кількість внутрішніх рівнів, що визначаються на основі аналізу $W_i \to IS$ і позначаються символом $r_i^{1t}(x_i)$ [105].

Діапазон рівня конфіденційності, який будемо позначати $r_i^{2t}(x_i)$ і в якому кількість рівнів визначається на основі аналізу $An_i(W_i)$, є діапазон, що характеризується наступним. Система алгоритмів, що використовується у цьому діапазоні, представляє собою алгоритми Ad_i, які формують результат своєго функціонування у дискретній формі. Результат при використанні Ad_i визначається на дискретній множині [106].

На основі представлених Za_i даних про $C_i(Za_i)$, вхідних даних $d_w(x_i)$ та обґрунтування необхідності використання даних типу $r_i^{2t}(x_i)$, система SNP проводить ряд перевірок, які є спільними для всіх рівнів $r_i^{2t}(x_i)$ та реалізує ряд процесів, що відображають специфіку рівня r_i^{2t}. Як і на попередньому рівні, необхідні дані розпізнаються по їх інтерпретаційних описах, які формуються в задачі та присутні в IS. У цьому випадку для перевірки допустимості використання $r_i^{2t}(x_i)$ в процесі розв'язання задачі використовуються алгоритми, які є аналогічними до алгоритмів Az_i, але результат проведеного аналізу такі алгоритми формують в дискретній формі. Це означає, що алгоритм Ad_i надає задачі інформацію про те чи можна використовувати відповідні дані, чи ні, на відміну від рівня $r_i^{1t}(x_i)$, у якому алгоритм Az_i надав задачі можливість використання x_i, але при цьому, надане значення x_i було замінене на значення, рівень конфіденційності якого є меншим. Алгоритм Ad_i, про який йде мова, аналогічно до алгоритму Az_i, реалізує своє функціонування на основі аналізу $An_i(W_i)$, які мають більш високий рівень небезпеки для функціонування W_i. Алгоритм Ad_i використовує дані типу $r_i^{2t}(x_i)$ таким чином, щоб результат його роботи допускав дискретну інтерпретацію і був узгоджений з Za_i. У більшості випадків, Ad_i дозволяє використовувати задачі Za_i дані типу $r_i^{2t}(x_i)$ у тому випадку, коли задача орієнтована на протидію $An_i(W_i)$ або Za_i орієнтована на елімінацію відповідної $\mathcal{K}r_i(W_i)$. Другою відмінністю роботи

Ad_i по відношенню до Az_i є те, що система SNP вимагає, щоб розв'язок задачі Za_i активізувався в середовищі IS або у спеціально виділеному окремому обчислювальному середовищі [107].

Функціонування SNP при аналізі даних з рівнем конфіденційності, який позначається $r_i^{3t}(x_i)$ і який може мати певну кількість рівнів конфіденційності, полягає у наступному. Так само як і в попередніх випадках, алгоритми Ar_i, які є аналогічні до Az_i і Zd_i, аналізують характеристики задачі Za_i. Основними компонентами цих характеристик є ціль задачі $C_i(Za_i)$, вхідні дані задачі Dw та схеми перетворень, що реалізуються в алгоритмі розв'язання Za_i, що відносяться до перетворень з даними $r_i^{3t}(x_i)$. У результаті такого аналізу алгоритм Ar_i формує ряд умов про допустимість використання в Za_i даних $r_i^{3t}(x_i)$. На відміну від перших двох діапазонів рівня конфіденційності, при виявленні запиту на конфіденційні дані третього рівня, які відповідають найбільш важливим даним, що стосуються предметної області (W_i), система SNP перевіряє обґрунтованість використання таких даних. Їх необґрунтоване чи, тим більше, несанкціоноване використання, може привести до значних втрат у середовищі W_i. Тому безпосереднє використання таких даних тією чи іншою задачею Za_i повинно перевірятися не тільки на допустимість, а й на обґрунтованість розв'язання такої задачі.

Обґрунтованість розв'язання задачі перевіряється наступним чином:

– перевіряється, чи у відповідності з параметрами Za_i у результаті розв'язання задачі Za_i не формуються передумови виникнення негативних ситуацій в результаті розв'язання інших санкціонованих задач в області W_i;

– перевіряється, чи безпосереднє використання відповідних даних в Za_i, при несуперечній меті, не призведе до опосередненого розкриття інформації про відповідні конфіденційні дані.

Оскільки рівень конфіденційності пов'язується з рівнем можливої небезпеки, до якої може призвести використання даних, то SNP повинна провести аналіз зовнішніх, по відношенню до IS і W_i, факторів, що можуть взаємодіяти з $IS \cup W_i$ або мають відношення до цього комплексу. Перевірка зовнішніх факторів полягає у

виявленні зв'язків між зовнішніми факторами та результатами розв'язання задачі, що описуються метою.

Передумова виникнення негативних факторів означає, що в W_i і IS сформувалася на логічному рівні структура, яка може виступити активізатором виникнення критичних ситуацій. Загалом це означає наступне. Нехай відомо, що $An_i(W_i)$ виникає у випадку, коли в системі можливий наступний вивід або послідовність дій та відповідних подій: $\forall Za_i \exists Za_j[(Za_j \& Pp_i(W_i)) \rightarrow An_i(W_i)]$, де Za_i – одна з задач, яка при використанні Pp_i може призвести до виникнення $An_i(W_i)$, яка має найвищий рівень небезпеки аномалії з точки зору її критичності, Pp_i – передумова, яка описується логічною формулою, що виникає в W_i.

Оскільки всі $\mathcal{K}r_i(W_i)$ або $An_i(W_i)$ задаються при формуванні IS і відповідної системи W_i, то існує можливість провести обернений вивід з метою виявлення деякої Pp_i [108, 109]. Якщо Pp_i буде виведено на основі параметрів задачі та $An_i(W_i)$, то SNP відмовить у наданні $r_i^{3t}(x_i)$ задачі Za_i, що буде відповідати першій перевірці.

Відомо, що процес розв'язання задачі Za_i, який потребує вхідні дані Dw, використовує не тільки значення цих даних, а і їх інтерпретацію. У більшості випадків інтерпретація вхідних даних відображається або використовується при проектуванні алгоритму Al, який передбачає використовувати ці дані. У рамках системи IS і, відповідно, W_i, крім самих величин значень даних використовуються текстові описи їх інтерпретації, що є необхідними компонентами бази IS. Інтерпретаційні описи конфіденційних даних, що описуються у вигляді $j[r_i^{3t}(x_i)]$ і використовуються для запиту цих даних, представляють собою опис певного їх наближення. Цей наближений опис є відомим для $K_i(Za_i)$. Доповнення такого опису реалізується фрагментом алгоритму Al_{ji}, що знаходиться в SNP. Відповідні перетворення не обов'язково призводять до виявлення повної інформації про $r_i^{3t}(x_i)$. Тому виникає задача перевірки, чи $j(r_i^{3t}(x_i)) \& j(al_i(r_i^{3t}(x_i))$ не призведе до повного виявлення інформації про $r_i^{3t}(x_i)$, або $J[r_i^{3t}(x_i)]$, у випадку, коли на основі описів $j[r_i^{3t}(x_i)]$ та $[al_i(x_i)]$ можна було б отримати вивід, що описується

співвідношенням: $\{j[r_i^{3t}(x_i)]\&j[al_i(x_i)]\} \to J[r_i^{3t}(x_i)]$, де $J[r_i^{3t}(x_i)]$ – є повним інтерпретаційним описом конфіденційних даних $r_i^{3t}(x_i)$ з IS. Якщо такий вивід є можливий, то відповідні дані переходять до статусу відкритих даних. Такий перехід може бути недопустимим, якщо в рамках W_i не реалізувалися перетворення, які унеможливили б виникнення відповідної аномалії в W_i. Очевидно, що будь-яке використання конфіденційних даних $r_i^{3t}(x_i)$ для реалізації деякого процесу $\Pr_i$, що породжується алгоритмом Al_i, призводить до пониження конфіденційності відповідних даних на певну величину $\delta[r_i^{3t}(x_i)]$. Щоб уникнути таких наслідків використання $r_i^{3t}(x_i)$, необхідно відповідні процеси $\Pr_i(Al_i)$ реалізовувати в умовах, які забезпечують відповідний рівень конфіденційності. Цей метод реалізується у рамках даного підходу за рахунок використання внутрішніх алгоритмів Az_i, які використовуються в якості фрагментів $Al_i \in Za_i$. Але це не може повною мірою гарантувати не розкриття даних $r_i^{3t}(x_i)$, оскільки в рамках реалізації процесів $\Pr_i(Al_i)$ можуть існувати процеси міграції інформації про вхідні дані і, у тому числі, про конфіденційні дані. Дослідження процесів міграції інформації про конфіденційні дані, чи про дані взагалі, які будемо позначати $Im[r_i^{3t}(x_i)]$ потребують окремого розгляду. Тому приймемо, що використання конфіденційних даних для розв'язання задач, призводить до певного рівня пониження їх конфіденційності. Визначення величини пониження рівня конфіденційності за рахунок міграції $Im[r_i^{3t}(x_i)]$ в рамках даної роботи визначається на основі використання системи прийняття рішення (SPR). У SPR формуються умови та правила, що застосовуються для реалізації процедур виводу певних рекомендацій у випадку, коли величини пониження рівня конфіденційності за рахунок міграції $Im(x_i)$ є не допустимими.

У рамках даного підходу існує також можливість компенсувати пониження рівня конфіденційності, що в багатьох випадках уникнути не можливо, наступним чином. Згідно з прийнятим положення про те, що рівень конфіденційності визначається рівнем загрози чи небезпеки, до якої може допровадити несанкціоноване використання конфіденційних даних в W_i, пониження рівня

конфіденційності даних можна допустити, якщо рівень відповідної небезпеки у необхідній мірі понизити шляхом її часткової елімінації. Цей підхід пов'язаний з необхідністю аналізу предметної області інтерпретації W_i. Тому цю задачу більш детально розглядати не будемо. Приймемо наступне положення.

Положення 3.3. Кожне використання конфіденційної інформації призводить до пониження рівня її конфіденційності, як мінімум, за рахунок міграції інформації про ці дані у процесі, що реалізує розв'язок відповідної задачі.

У більшості випадків в середовищі W_i критичні ситуації призводять до негативних наслідків, коли вони активізуються тими чи іншими подіями. Серед таких подій можуть бути:

– події, що обумовлюються зовнішніми факторами, які не зв'язані безпосередньо з процесом $Pr_i[Za_i]$;

– події, що обумовлені процесом розв'язання окремої задачі, яка використовує конфіденційні дані;

– події, що обумовлюються саме активізацією аномалій An_i чи $\mathcal{K}r_i$ в W_i.

Приведені особливості переважно відносяться до системи прийняття рішень, і пов'язані з аналізом області W_i і тому більш детально розглядатися не будуть.

Розглянемо метод оцінки рівня конфіденційності даних. На загальному рівні відмітимо наступні положення, що стосуються оцінки конфіденційних даних. Така оцінка потрібна в основному для того, щоб можна було говорити про той чи інший рівень безпеки даних без використання кожного разу опису інтерпретацій величини рівня конфіденційності. Оцінка рівня конфіденційності $r_i(x_i)$ передбачає необхідність впровадження певної шкали вимірювань. Така шкала повинна бути відносною, оскільки конфіденційність як деяке поняття, є поняттям відносним. Оскільки уявлення про конфіденційність можна розглядати по відношенню до уявлень про величини втрат при несанкціонованому використанні конфіденційних даних для розв'язання деякої задачі Za_i, то величину рівня конфіденційності доцільно визначати у зв'язку з величиною можливих втрат. Для цього необхідно ввести наступні положення та визначення, що стосуються цих питань.

Положення 3.4. Оскільки будь-які дані, у тому числі, й конфіденційні, мають свою предметну область інтерпретації W_i, то параметри, що використовуються для опису цих даних, також повинні мати інтерпретацію в цій же предметній області.

Визначення 3.9. Довільна предметна область W_i, яка розглядається у даному випадку, представляє собою сукупність окремих об'єктів $\{y_i\}$, об'єднаних у певну структуру $S(X)$, яка може представлятися на графовому та логічному рівнях $G(Y)$ і $L(Y)$ відповідно, а також сукупність процесів $Pr_i(Y)$, які реалізуються у відповідних структурах записується у вигляді:

$$W_i = \{G(Y), L(Y), Pr_i(Y)\}$$

Втрати, які можуть мати місце в W_i, обумовлюються виникненням аномалій $An_i(W_i)$ або виникненням критичних ситуацій $\mathcal{K}r_i(W_i)$.

Визначення 3.10. Кожна W_i функціонує відповідно до деякої стратегії або сукупності стратегій $St(W_i)$, які реалізуються на основі використання процесів Pr_i.

$$St(W_i) = F(Pr_i, \dots, Pr_m),$$

де F – функція взаємозв'язків між Pr_i та Pr_m.

Визначення 3.11. Аномалією $An(W_i)$ є така зміна в середовищі W_i, що призводить до неможливості реалізації окремих процесів.

$$An(W_i) \to St(Pr_1, \dots, \neg Pr_i, \dots Pr_m).$$

Визначення 3.12. Критичною ситуацією $\mathcal{K}r_i(W_i)$ є така зміна в середовищі W_i, яка призводить до неможливості реалізації однієї із стратегій.

$$Kr_i(W_i) \to \{St_1 * \dots * \neg St_i * \dots * St_m\}.$$

Для використання приведених визначень при формуванні оцінки величини конфіденційності необхідно ввести наступні умови та обмеження.

Умова 3.1. Діапазон вимірювання величини конфіденційності окремих даних буде представляти собою шкалу від нуля до 100, а одиницею вимірювання величини конфіденційності приймемо величину процентів.

Введемо наступні положення.

Положення 3.5. Приймаємо, що можуть існувати алгоритми розв'язання задачі або відповідних задач Za_i, орієнтованих на досягнення мети, що полягає у впровадженні втрат в об'єкті або предметної області, де задача має інтерпретацію.

Положення 3.6. Можуть існувати задачі, орієнтовані на мету, що полягає у розвитку предметної області W_i та протидії можливим негативним факторам, дія яких на W_i у рамках предметної області має власну інтерпретацію.

Визначення 3.13. Рівень конфіденційності даних $r_i^t(x_i)$ визначається величиною втрат, до яких може призвести реалізація задачі, метою якої є безпосередня або опосереднена дія на W_i, яка призведе до втрат, розмір яких можна визначити.

Визначення розміру втрат полягає в аналізі наступних факторів, що можуть мати місце в середовищі W_i:

– неможливість реалізації окремого процесу або групи процесів $\{Pr_{is}, \dots Pr_k\}$;

– неможливість реалізації однієї із стратегій $St_i(W_i)$;

– елімінація компоненти x_i з X та інші зміни в W_i, які можуть мати негативну інтерпретацію в довільній із стратегій St_i, які визначаються в W_i.

Очевидно, що одні і ті ж дані можуть використовуватися для реалізації задач позитивного впливу і негативного впливу на W_i. Рівень позитивного впливу, який здійснює реалізація задачі Za_i, може визначати величину конфіденційності даних, з використанням яких такий вплив здійснюється. Незалежно від цього, величина рівня конфіденційності визначається величиною втрат при можливості реалізації негативного впливу на W_i [110]. Величина негативного впливу суттєво залежить від конкретної предметної області та її особливостей. На загальному рівні величина негативного впливу на W_i визначається наступним чином:

– у діапазоні конфіденційності r_i^{1t} – визначається кількістю елементів $\{x_i\}$, до елімінації яких приводить негативний вплив;

– у діапазоні конфіденційності $r_i^{2t}(x_i)$ – визначається кількістю аномалій, до виникнення яких приводить негативний вплив;

– у діапазоні конфіденційності r_i^{3t} – визначається кількістю критичних ситуацій, до яких призводить негативний вплив.

Всі наведені величини вимірюються в процентах від всього об’єму відповідних факторів, що мають місце у W_i в цілому. Весь діапазон значень у процентах ділиться

на три діапазони, які виділяються для трьох діапазонів конфіденційності даних з W_i. Такий поділ є наступним:

– від 0% до 50% – використовується для визначення підрівнів конфіденційності в діапазоні r_i^{1t};

– від 50 % до 80% – використовується для визначення підрівнів конфіденційності в діапазоні r_i^{2t};

– від 80% до 100% – використовується для визначення підрівнів конфіденційності в діапазоні r_i^{3t}.

Такий розподіл шкали рівня конфіденційності ґрунтується на тому, що унеможливлення окремих стратегій приносить максимальні втрати і коли унеможливлено виконання всіх стратегій, то втрати приймають величину 100%. Втрати окремих процесів визначаються у діапазоні від 50% до 80%. При цьому, якщо кількість втрачених процесів відповідає втраті однієї St_r, то процент стає рівний величині, яка відповідає втраті одного St_i в діапазоні від 80% до 100%. Аналогічно існує зв'язок втрат елементів $x_i \in r_i^{3t}(x_i)$ з втратами окремих процесів. З цього виходить, що шкала визначення r_i^t не лінійна і є різною для різних W_i.

Висновок до розділу 3

У третьому розділі проводяться дослідження, що ґрунтуються на аналізі окремих факторів, що впливають на безпеку системи доступу в цілому. Завдяки цьому стало можливим розглянути задачу реалізації процесів функціонування основних компонент моделі системи доступу, яка їх об’єднує. Тому у роботі розглядаються основні компоненти моделі захисту системи доступу.

Модель захисту доступу, в основному, ґрунтується на використанні системи надання повноважень. У зв’язку з цим введено визначення аномалій, які можуть мати місце в IS, що стосуються системи IS в цілому та уявленя про негативні фактори, що можуть виникати в предметній області інтерпретації даних з IS. Доводиться твердження про умови виникнення суперечностей у процесах, які виникають у цій предметній області в результаті розв’язання прикладних задач, результати розв’язання яких використовуються в предметній області інтерпретації.

Вводиться визначення актуальності прикладної задачі та розглядаються методи визначення величини цього параметру.

Досліджуються методи обчислення рівня безпеки системи, які розглядаються в аспектах забезпечення захисту, що обумовлюється використанням системи надання повноважень. У рамках цього дослідження проводиться аналіз всієї сукупності параметрів, що використовуються в рамках системи надання повноважень та IS в цілому.

У роботі доводиться можливість розпізнавання рівня конфіденційності даних, за якими звертається прикладна задача до системи надання повноважень.

Досліджуються основні компоненти дворівневої системи захисту доступу до IS.

РОЗДІЛ 4 Реалізація основних компонент системи надання повноважень

4.1 Розробка та аналіз процесів надання повноважень

Алгоритм надання повноважень (ANP) реалізує всі операції, необхідні, для реалізації процесу доступу до конфіденційних даних. Користувач після отримання доступу до системи вводить необхідні дані про задачу Za_i і фрагменти алгоритму її реалізації, які потребують конфіденційну інформацію для свого функціонування. Таким чином, не залежно від користувача задача Za_i безпосередньо ідентифікується в системі надання повноважень для отримання даних. Запит потрібних даних представляє собою текстові описи їх інтерпретації $D_w^z = [(x_i^z), \dots, j(x_{ik}^z)]$. Система SNP містить, крім самих даних, не тільки їх значення, а й інтерпретаційні описи цих даних $D_i^s = [j(x_1^s), \dots, j(x_m^s)]$ [111]. Система SNP по $j(x_1^s)$ визначає відповідні дані $j(x_{i1}^s)$. На основі інтерпретаційного опису $j(x_i^z)$ система визначає відповідні параметри даних. Наприклад, якщо має місце $\sigma[j(x_1^s) * j(x_i^z)]$, які семантично відрізняються більше ніж на $\delta\sigma$, пошук даних продовжується. Якщо серед всіх даних типу r_i^t вибрано дані, що задовольняють вимогам вибору, встановлюються базові параметри даних.

До таких параметрів відносяться наступні параметри даних:

- рівень конфіденційності даних $r_i^{kt}(x_i)$;
- рівень значимості даних $\aleph_i(x_i)$;
- рівень обґрунтованості використання даних $\lambda_i(x_i)$.

Перевірка параметру $\lambda_i(x_i)$ дозволяє викрити системі SNP спробу несанкціонованого вибору даних $r_i^{kt}(x_i)$. Якщо в результаті семантичного аналізу $\sigma[j(x_1^s) * j(x_i^z)]$ вибрано деякі дані $[r_i^{kt}(x_i^z) * r_i^{kt}(x_i^s)]$, перевіряється параметр конфіденційності Za_i, якщо ці параметри відрізняються більше, ніж на задану величину $\Delta(r_i^{kt})$ то повноваження відповідній Za_i на отримання даних не надаються. Параметр $\aleph_i(x_i^s)$ в процесі функціонування IS змінюється, оскільки він визначається частотою його використання на заданому інтервалі часу ΔT. Рівень

відмінності між $\aleph_i(x_i^z)$ та $\aleph_i(x_i^s)$ задається величиною $\Delta\aleph_i$. Перевірка параметру $r_i^{kt}[x_i(x_i^z)]$ є специфічною, оскільки, для його визначення використовуються дані, отримані у результаті використання $r_i^{kt}[x_i(x_i^s)]$ задачею Za_i, які розміщаються в описі мети розв'язання задачі $C(Za_i)$ [112].

У процесі перевірки умов надання повноважень Za_i може виявитися, що $r_i^t(x_i^z) \neq r_i^t(x_i^s)$ більше, ніж на $\sigma(r_i^t)$. У цьому випадку система SNP може вибрати дані, які відповідають вказаному значенню параметра r_i^t за умови, що $r_i^t(x_i^z) \ll r_i^t(x_i^s)$, де знак $\ll$ – означає нижчий діапазон значень конфіденційності даних. Після цього SNP перевіряє, чи $C_i[Za_i(r_i^{*t}(x_i))]$ відповідає меті, заданій у параметрах задачі. Якщо така відповідність існує, то задача отримує по цьому параметру дозвіл на використання даних, у яких $[r_i^{kt}(x_i)\&(k \ll m)]$, де k – рівень діапазону конфіденційності, який вибрала система SNP, m – рівень діапазону конфіденційності, який замовляла задача. Така ситуація є можливою, оскільки текстова інтерпретація даних $j(x_i^z)$, які замовляються Za_i, не відповідає повною мірою текстовій інтерентитації $j(x_i^s)$, яка розміщається в системі. Така невідповідність може призвести до того, що дані будуть вибрані з нижчого діапазону конфіденційності [113].

Така ситуація може обумовлюватися наступними причинами:

– рівень конфіденційності в IS для даних x_i^z міг зменшитися в силу різних відомих причин;

– інформація про дані у користувача може бути не точна, оскільки предметна область інтерпретації, якою є певне середовище описується з певним наближенням.

При виборі даних, за якими звернулася задача до системи SNP, остаточне рішення з надання тих чи інших даних, SNP приймається на основі даних аналізу всіх контрольованих параметрів, якими є $\{r^t, \aleph_i, \lambda_i\}$ [114].

Система SNP при наданні повноважень Za_i реалізує не тільки аналіз параметрів даних, а й аналіз параметрів самої задачі Za_i. Першим параметром, який перевіряється, є параметр суперечності мети розв'язання задачі з іншими компонентами, що надаються користувачем при пред'явлені задачі. Компоненти

представляють собою її логічний опис, який є з відповідним їх наближенням. Наприклад, компонентами можуть бути алгоритм задачі $Al_i \in Za_i$, мета задачі. Якщо остання представляє собою деяку конструкцію, наприклад, створення деякого фрагменту для W_i, то такою компонентою є логічний опис цієї конструкції або параметри вихідних даних, якщо мета $C_i(Za_i)$ передбачає тільки перетворення вхідних даних. Наявність суперечності свідчить про неконкретне формулювання задачі і тоді SNP відмовляє у наданні повноважень до використання даних.

Рівень конфіденційності задачі повинен бути узгоджений з рівнем конфіденційності вхідних даних D_w і особливо, вихідних даних (D_ϑ). Очевидно, що $r^t(D_w) \geq r^t(D_\vartheta)$. У більшості задач Za_i, що стосуються окремих середовищ, виконується приведене співвідношення. На величину $r^t(D_v)$ впливає такий фактор, як міграція даних $(Im(x_i))$ з входу $Al(Za_i)$ до виходу процесу розв'язання задач, яким є $C_i(Za_i)$. Міграція полягає у збереженні ключових елементів опису інтерпретації даних $I(D_w) = j(x_s^w), \dots, j(x_m^w)$ по відношенню до $I(D_v) = j(x_i^v), \dots, j(x_k^v)$. Очевидно, що рівності $I(D_w)$ і $I(D_v)$ досягнути не можливо, але рівень відповідності цих двох компонент визначає величину міграції інформації в процесі розв'язання задачі Za_i. Можна було б припустити, що об'єднання даних з різними параметрами конфіденційності, призведе до того, що рівень конфіденційності результату буде вищий. Ця обставина визначається на основі інтерпретації алгоритму розв'язання задачі і задається параметром рівня конфіденційності самої задачі $r^t(Za_i)$. Цей параметр перевіряється системою SNP і враховується при наданні повноважень доступу до даних. Автор програми повинен сам визначати рівень конфіденційності самої програми, яку він проектує. Обґрунтування рівня конфіденційності для програми за аналогією з рівнем конфіденційності даних пов'язане з аналізом величини втрат, до яких може призвести несанкціоноване використання такої програми. При такій інтерпретації визначення рівня конфіденційності спроектованої задачі або спроектованого алгоритму слід визначати по величині втрат, до яких може призвести несанкціоноване використання розв'язання задачі. Виходячи з цього, можна було б ввести інтегральний критерій вибору задач, які не потребували б для своєї

характеристики параметру конфіденційності. Але в цьому випадку може виникати протиріччя, яке полягає у наступному. Дані, що можуть потребувати параметр певного рівня конфіденційності, виникають не завжди в результаті діяльності людини, а можуть виникати в окремих випадках на основі досліджень в галузях природничих наук. Наявність такого типу конфіденційних даних обумовлює можливість, а у багатьох випадках і необхідність створювати алгоритми і розв'язувати задачі, які необхідно характеризувати параметрами конфіденційності.

Значимість задачі в рамках SNP визначається порівняно просто. Проводиться аналіз величини змін, які переважно описуються в меті задачі $C_i(Za_i)$, які відбудуться в W_i в результаті використання розв'язання Za_i. Величина змін визначається:

– по кількості елементів x_i, які будуть впроваджені $m^x(x_i)$ в W_i;

– по кількості процесів, які будуть впроваджені в W_i або $m^p(Pr_i)$;

– по кількості аномалій, які будуть ліквідовуватися в W_i, у результаті розв'язання задачі $m^a(An_i)$;

– по кількості критичних ситуацій, які передбачається ліквідувати у результаті розв'язання Za_i або $m^K(\mathcal{K}r_i)$.

Кожний з коефіцієнтів m^x, m^p, m^a та m^k має власне значення або вагу, яка відображає значимість результатів розв'язання Za_i для функціонування W_i. Така значимість змінюється у відповідності із співвідношенням $m^x < m^p < m^a < m^k$. У випадку коефіцієнтів m^x та m^P мова може йти не тільки про збільшення x_i та m^P, а і про зменшення їх в W_i, якщо це не призведе до зменшення параметру актуальності $Ak(Za_i)$ відповідної задачі. Якщо в рамках однієї задачі реалізуються зміни кількості x_i в W_i, зміни кількості $Pr_i \in W_i$ чи елімінація An_i, то значення параметру $\aleph(Za_i)$ визначається наступним співвідношення:

$$\aleph(Za) = m^x + m^{Pr} + m^a.$$

У більшості випадків, елімінація критичних ситуацій $\mathcal{K}r_i$ реалізується окремими Za_i, оскільки такі задачі в рамках системи $(IS\&W_i)$ мають найвищий пріоритет.

Актуальність задачі $Ak(Za)$ для своєго визначення потребує додаткових даних про W_i в IS. Одним з класів таких даних є критерії прогресивності змін, до яких призводить використання результатів Za в W_i. Критерії прогресивності змін в W_i можна отримувати на основі використання еволюційних моделей [115] прикладом якої може служити модель, що використовує генетичні алгоритми [116, 117]. За своєю природою IS є базою даних і, тому вводити в IS алгоритми типу генетичних не достатньо коректно. У зв'язку з цим, приймемо критерії, якими будемо визначати прогресивність кожної окремої задачі, яка використовує конфіденційні дані.

Перш ніж формулювати критерії, підкреслимо, що всі дані, які знаходяться в IS є елементами W_i, яку IS обслуговує. Результати процесу розв'язання задачі Za_i можуть бути елементами, які будуть включатися до складу W_i і, відповідно, будуть розширяти IS_i. Формулювання критеріїв, переважно, полягає у порівнянні щонайменше двох факторів і на основі такого порівняння реалізується вибір одного з факторів. Система IS_i містить дані з W_i, яке є джерелом вхідних даних, що може використовуватися при порівнянні для формування критеріїв. Передбачувані результати розв'язання задачі описуються у певному наближенні в описі мети задачі. Тоді критерії можуть ґрунтуватися на результатах аналізу мети задачі та даних, отриманих в результаті її розв'язання, і порівнянні даних отриманих результатів аналізу. Сформулюємо ряд критеріїв та обґрунтуємо їх доцільність.

Критерій 4.1. Якщо в результаті перетворень, які реалізуються алгоритмом $Al_i(Za_i)$ задачі Za_i, рівень конфіденційності вихідних даних є нижчим порівняно з рівнем конфіденційності вхідних даних, відповідні перетворення Za_i можна вважати актуальними.

У відповідності з прийнятими положеннями, необхідність використання конфіденційних даних обумовлюється тим, що останні можуть бути використані для реалізації негативного впливу на W_i, наприклад, для формування в W_i аномалій $An_i(W_i)$. Зниження рівня конфіденційності даних, як і зменшення кількості конфіденційних даних, які описують деяку W_i допускає інтерпретацію відповідних перетворень як прогресивних, оскільки такі зміни в даних призводять до зменшення можливості реалізації негативного впливу на W_i і, відповідно на IS.

Критерій 4.2. Якщо результатом розв'язання Za_i є нове правило перетворень, що передається в W_i, яке не призводить до суперечностей в існуючій системі правил перетворень, відповідну задачу Za_i можна вважати актуальною.

У будь-якому середовищі або достатньо складному об'єкті завжди реалізуються ті чи інші процеси, особливо, коли мова йде про соціальні середовища, на обслуговування яких орієнтована система IS. Процеси реалізуються на основі використання перетворень, система яких повинна бути не суперечна. Якщо система правил перетворень розширюється новим перетворюванням, яке не призводить до виникнення суперечності у відповідній системі, останнє сприяє можливості функціонального розширення існуючих процесів і може сприяти можливості реалізації нових процесів. Розширення асортименту можливих процесів, що відбуваються в W_i допускає інтерпретацію еволюційного розвитку відповідної системи.

Критерій 4.3. Якщо в результаті передачі розв'язання задачі Za_i в систему W_i, в останній елімінується аномалія, така задача приймається прогресивною.

Цей критерій не потребує додаткових коментарів, а його використання та виділення в окремий критерій ґрунтується на тому, що аномалія $An_i(W_i)$ може існувати в W_i і певний час не призводити до порушень у поточні моменти процесу функціонування. Тому відповідна задача визначається як актуальна.

Критерій 4.4. Якщо в результаті розв'язання задачі Za_i, до W_i додається деяка компонента $\varphi_i(x_{is}, \dots, x_{ik})$, яка представляє собою деяку структуру, що не є суперечною із структурами вхідних даних Dw_i та структурами предметної області W_i, відповідна задача Za_i допускає інтерпретацію прогресивної задачі.

Додавання до системи W_i, яка має власну структуру, деякої компоненти $\varphi_i(x_{is}, \dots, x_{ik})$, яка не призводить до виникнення в W_i суперечності, не тільки збільшує кількісно предметну область W_i, а і розширює її функціональні можливості, оскільки додаткова структура також може приймати участь у процесах функціонування, які уже реалізуються в W_i і тим самим їх змінювати або їх модифікувати. Такі зміни в W_i допускають інтерпретацію прогресивних,

еволюційних змін і тому відповідна задача може характеризуватися як актуальна в рамках W_i.

Слід відмітити, що параметр актуальності задачі $Ak(Za_i)$ має дискретний характер, що виникає з приведених критеріїв. Це означає, що цей параметр може інтерпретуватися як величина, значення якої визначається на деякому неперервному інтервалі. У випадку критерія 4.1 величина $Ak(Za_i)$ може вимірюватися кількістю конфіденційних компонент для яких був знижений рівень конфіденційності. У випадку критерія 4.2 актуальність вимірюється кількістю нових правил перетворень, які сформувалися в результаті розв'язання задачі Za_i, яких може бути більше одного. Тоді $Ak(Za_i)$ визначається на інтервалі, який описує максимальну кількість можливих правил перетворень.

У випадку критерію 4.3 кількість елімінованих аномалій може бути більше однієї. Тоді $Ak(Za_i)$ приймає ряд значень величин $Ak(Za_i)$, які відповідають кількості усунених аномалій An_i.

У випадку критерія 4.4 розмір компоненти може мати різну величину. Розмір компоненти в найпростішому випадку може вимірюватися кількістю елементів x_{ij}, які входять до її складу, що дозволяє величину $Ak(Za_i)$ визначити на відповідному інтервалі чисел. Крім того, такий інтервал визначення величини $Ak(Za_i)$ може бути збільшений на кількість процесів у яких відповідна компонента приймає участь в рамках середовища W_i.

Розглянемо загальний параметр безпеки задачі $\eta(Za_i)$. Цей параметр необхідний, насамперед для оцінки загальної величини небезпеки, яка обумовлюється розв'язанням задачі Za_i. При цьому не проводиться оцінка різних режимів реалізації розв'язання задачі, наприклад, режимів, що відповідають помилковим розв'язанням чи відсутності розв'язання. Приймається, що задача є сформульована коректно, а алгоритм Za_i розв'язання цієї задачі побудовано таким чином, що всі варіанти розв'язання задачі, що відтворюються в Al_i є коректні та обґрунтовані. Крім того приймемо, що мета задачі не орієнтована на створення аномалії в W_i і, тим більше, не орієнтована на активізацію критичної ситуації в W_i. У даному випадку під коректною задачею будемо розуміти таку задачу, яка

характеризується параметрами важливості або значимості задачі $\aleph_i(Za_i)$ та параметрами її актуальності $Ak(Za_i)$.

Небезпека задачі Za_i або $Nb(Za_i)$ може носити характер безпосередній та опосередкований. Безпосередній характер безпеки задачі $\eta^b(Za_i)$ полягає у тому, що при передачі результатів розв'язання Za_i в середовище W_i відразу виникають негативні фактори, щонайменше у вигляді аномалій різного типу $An(W_i)$.

Розглянемо завдяки чому може мати місце ситуація, коли $\eta(Za_i) \neq max$. Величина $\eta(Za_i)$ задається в діапазоні $[\alpha\beta]$ де $\beta = max\,\aleph(Za_i), \alpha = min\,\aleph(Za_i)$. Приймаємо, що алгоритм $Al(Za_i)$ та мета $C_i(Za_i)$ сформовані коректно. Тоді відхилення $\aleph_i(Za_i)$ від максимального значення може виникнути через наступні причини.

Вхідні дані в Za_i задаються шляхом надання $\{j(x_{is}), \dots, j(x_{ik})\}$, де $j(x_{ik})$ – текстовий опис даних, які не можуть абсолютно адекватно їх описувати. Тому вхідні дані, які отримує Za_i, будуть давати похибку ΔDw_i.

Аналогічно і мета $C_i(Za_i)$ не може описувати результат розв'язання абсолютно точно, бо інакше не потрібно було б таку задачу розв'язувати. Внаслідок цього виникає похибка типу $\Delta C(Za)$. Аналогічну ситуацію створює компонента, що представляє собою $Al(Za_i)$, а помилка яку допускає алгоритм, буде давати відхилення $\Delta Al(Za_i)$. Тоді загалом рівень безпеки можна записати наступним чином:

$$\eta(Za_i) = \delta[f(\Delta Dw, \Delta R, \Delta Al)].$$

З цього співвідношення виходить, що з ростом ΔDw, ΔR і ΔAl рівень безпеки $\eta(Za_i)$ зменшується. Розглянемо причини, через які $\eta(Za)$ не може бути максимальним. Коли задача Za_i отримує вхідні дані Dw з IS, то в силу того, що ці дані вибираються на основі семантичного аналізу $\{[j(x_{is}^z), \dots, j(x_{ik}^z)]\&[j(x_{is}^s), \dots, [j(x_{ik}^s)\}$ відповідні значення Dw будуть надані з похибкою ΔDw, оскільки семантичний опис x_i^z може не завжди співпадати з необхідною точністю з описом даних, які знаходяться в IS або x_i^z. Мета задачі $C_i(Za_i)$, у якій описуються вихідні дані, також не може бути описана достатньо

точно, інакше не було б сенсу розв’язувати задачу. Рівень безпеки задачі $\aleph_i(Za_i)$ є тим вищий, чим більш точно розв’язання задачі відповідає меті. Це свідчить про те, що рівень безпеки задачі по параметру $\Delta C_i(Za_i)$ ніколи не буде максимальним. Величина $\Delta C_i(Za_i)$ привносить певний [118, 119] вклад у пониження рівня безпеки. Алгоритми задач, які реалізують процеси їх розв’язання, не можуть достатньо точно відображати ті процеси, які описує розв’язання задачі. Будь-який алгоритм процесу функціонування, що має природний характер, чи процесу, що має технічний характер та інші процеси, описуються з певними наближеннями до своїх реальних процесів, які вони моделюють [120]. Тому вони не можуть бути абсолютно адекватним відповідному процесу. Це призводить до відхилення $\Delta Al(Za_i)$. Якщо дотримуватися інтерпретації поняття безпеки задачі, яке представляється як спосіб забезпечення максимальної точності розв’язання, можна стверджувати, що абсолютно адекватного способу розв’язання задачі досягнути неможливо.

У багатьох випадках аспекти, про які йшла мова вище, впливають на точність розв’язання задачі [121, 122]. У нашому випадку точність розв’язання задачі впливає на рівень безпеки системи, яка використовує отримані результати. Тому у даній ситуації ми мусимо керуватися не тільки точністю її розв’язання, а інтерпретацією отриманих результатів з точки зору вимог до безпеки об’єкту, для якого задача проводить обчислення. Це означає, що необхідна точність розв’язання задач визначається рівнем безпеки.

Розглянемо можливий зв'язок рівня безпеки задачі $\eta(Za_i)$ з точністю розв’язання. Кожна задача Za_i, що розв’язується в рамках співпраці з IS_i, орієнтована на певний процес або на певний фрагмент з предметної області W_i. Це означає, що необхідна точність формується як одна з початкових умов проектування процесу розв’язання відповідної задачі. Відповідно до умови, яка визначає необхідну точність, вибираються основні характеристики задачі, до яких відносяться:

– тип алгоритму розв’язання задачі Al;
– допустима неточність вхідних даних (Dw).

Незважаючи на попередній вибір параметрів, що визначають точність реалізації розв'язання задачі, у силу причин, які були описані вище, необхідна точність може виявитися не забезпеченою. При роботі з реальними об'єктами, на потреби яких створюється IS та розв'язуються ті або інші задачі, у більшості випадків, немає можливостей організувати повторне проектування задачі, а також часто немає можливостей повторно розв'язувати саму задачу, наприклад, змінивши її вхідні дані чи інші параметри, що піддаються швидкій зміні. У цьому випадку, користувач отримує результати такі, які вдалося отримати і виникає задача оцінки рівня безпеки їх використання у предметній області W_i. У цьому випадку мова йде про те, що користувач отримує певне рішення і самостійно пробує його використати в W_i. Переважно W_i функціонує на основі використання інформаційно-управляючих засобів, з якими співпрацюють системи типу IS. Тому результати розв'язання задач, що орієнтовані на використання в W_i, недоцільно замикати на користувача, як на особу, що безпосередньо реалізує впровадження. Доцільно результати розв'язання задач, які можна було б реалізувати в системах з середовища W_i, доповнити інформаційними управляючими системи безпосередньо в W_i. У цьому випадку, можна було б автоматизувати процеси визначення рівня безпеки задачі або $\eta(Za_i)$. Очевидно, що у випадку, коли виявиться, що рівень безпеки недостатній, її результати не будуть використовуватися в рамках W_i. Інтерпретація недостатнього рівня безпеки Za_i може полягати у тому, що використання такого типу результатів може призвести до виникнення в W_i аномалій різного типу або може призвести до виникнення критичних ситуацій $\mathcal{K}r_i(W_i)$, що є недопустимим.

Приведене вище ілюструє той факт, що в інформаційних технологіях дослідження та розв'язання нових задач у дещо вузьких рамках сформульованої задачі, у більшості випадків, призводить до необхідності розширяти сферу впровадження отриманих результатів на суміжні системи, які є оточенням середовища, в якому проводяться дослідження. Підтвердженням цього є необхідність розширення розв'язання задач надання повноважень на використання, у даному випадку, конфіденційних даних до задач використання процесів, що

входять у відповідну систему в IS, а також в системах, які є предметною областю інтерпретації основної задачі.

Кількість параметрів, які можна використовувати для характеристики задач, можна розширити. Таке розширення може призвести до можливості отримання додаткових результатів у забезпеченні їх безпеки.

4.2 Аналіз умов та вимог до алгоритму надання повноважень задачам на використання даних

При розробці алгоритму надання повноважень необхідно реалізовувати процеси аналізу на основі використання числових даних параметрів, які при цьому використовуються. Це означає, що для всіх параметрів необхідно ввести способи визначення їх значень, ввести метрики вимірювання таких значень та узгодити шкали вимірювань різних параметрів. У системі SNP використовуються три групи параметрів, до яких відносяться:

– параметри конфіденційних даних:
– параметри задач, що потребують конфіденційні дані;
– загальні інформаційні параметри.

Крім аналізу методів визначення числових значень параметрів, необхідно визначити методи взаємного аналізу параметрів, які відносяться до IS з відповідними параметрами, що відносяться до задач, які звертаються до IS за отриманням даних.

Розглянемо параметри даних, якими є:

– рівень конфіденційності $r_i(x_i)$;
– рівень важливості $\aleph_i(x_i)$;
– рівень обґрунтованості їх використання $\lambda_i(x_i)$.

Рівень конфіденційності є величина, що визначається різними інтервалами значень, кожний з яких є певним рівнем конфіденційності. Інтервал між двома рівнями конфіденційності визначає рівень конфіденційності, величини яких є

меншими від більшої границі інтервалу. Величина інтервалів та кількість рівнів конфіденційності в них вибираються на основі інтерпретації втрат у предметній області інтерпретації, до яких призводить несанкціоноване використання відповідних даних. Для визначення таких рівнів можуть використовуватися різні масштаби, а кожний інтервал рівня конфіденційності може мати різну кількість відліку підрівнів конфіденційності. Це означає, що в цілому шкала величини параметру конфіденційності є не лінійна і для кожного інтервалу може бути різною. Різні дані, що відносяться до різних елементів W_i, можуть відноситися до різних підрівнів конфіденційності в рамках одного рівня. Деякі величини можуть мати однакові рівні конфіденційності і так далі. Зміна рівнів конфіденційності, яка визначається величиною втрат, реалізується зміною величини конфіденційності, що відповідає величині зміни відповідних втрат. Величина втрат може виявитися більша, ніж рівень конфіденційності у деякому інтервалі рівнів конфіденційності. Тому відповідні втрати приймаються більшими на стільки, щоб така втрата відповідала найближчому більшому рівню конфіденційності. Зменшення рівня конфіденційності, що відноситься до даних, які характеризують елемент в W_i, реалізується з дискретністю, яка передбачена встановленими величинами рівнів та підрівнів конфіденційності в кожному з прийнятих рівнів конфіденційності.

Рівень важливості $\aleph_i(x_i)$ є параметром, який на початковому етапі встановлюється у відповідності з проектними або прийнятими величинами, якщо W_i є технічним об’єктом чи об’єктом іншого типу, відповідно. Протягом процесу роботи IS відслідковується в рамках SNP частота використання відповідного x_i і залежно від цього, величина $\aleph(x_i)$ змінюється. При аналізі $\aleph(x_i)$, система SNP визначає чи величина $\aleph(x_i) \geq \delta_i\aleph$, де $\delta_i\aleph$ – величина порогу, меншим від якого $\aleph_i(x_i)$ не повинен бути.

Рівень обґрунтованості визначається на основі аналізу мети та значимістю x_i для досягнення мети $C_i(Za_i)$. У цьому випадку також використовується порогове значення, яке визначає різницю між $C_i(Za_i)$ та метою, яка досягається без використання x_i. У кінцевому випадку $\delta_i\aleph$ і $\delta_i\lambda$ приймаються, як величини безрозмірні [123, 124].

В IS всі дані характеризуються параметрами r_i, $\aleph_i$ і λ_i. Кожен з цих параметрів у процесі роботи SNP аналізується окремо. Якщо аналізовані параметри, значення яких представлені задачею Za_i або $r_i(x_i^z)$, $\aleph_i(x_i^z)$ та $\lambda_i(x_i^z)$ відповідають приведеним обмеженням, що задаються порогами, задача отримує доступ до значень відповідних даних, що приведені в рамках задач. Оскільки параметри, які потребує задача описуються у вигляді $j(x_i^z)$, а не адресами їх розміщення, дані розміщаються в IS у відповідності з їх текстовими описами. Це означає, що точність опису тих чи інших даних визначається повнотою інтерпретаційного опису у відповідному запиті, що надає задача Za_i системі SNP.

Функціональні зміни рівня конфіденційності обумовлюються причинами, що характеризуються процесами функціонування системи. Процеси функціонування системи IS полягають у реалізації наступних функцій:

– наданні даних різним типам задач і користувачам, що звертаються до системи за цими даними;

– аналіз запитів задач з точки зору обґрунтованості відповідних запитів;

– аналіз запитів на отримання даних з точки зору уповноважень, які мають задачі для їх використання;

– визначення поточного значення безпеки системи;

– управління рівнями та мірами конфіденційності даних.

У результаті надання конфіденційних даних, останні можуть змінювати свій рівень конфіденційності в силу наступних причин, що пов’язані з уявленнями про їх конфіденційність:

– відтворюваності вхідних конфіденційних даних шляхом використання оберненості алгоритму, що використовує вхідні дані;

– частота санкціонованого використання конфіденційних даних задачами, що звертаються за ними;

– час існування даних у рамках системи.

Оскільки приведені причини є незалежними, управління кожною з них, залежно від того, яка з цих причин на поточний момент є домінуючою, можна реалізовувати наступними способами.

Відтворюваність величин конфіденційних даних на основі аналізу алгоритмів, насамперед, визначається на основі інтерпретації всіх компонент, що реалізують перетворення конфіденційних даних у даному алгоритмі. Формально це описується співвідношенням:

$$j(Al_i) = j(al_{i1}) * j(al_{i2}) * \ldots * j(al_{im}), al_{ij} \in Al_i \quad (4.1)$$

Введемо наступне визначення.

Визначення 4.1. На рівні інтерпретації оберненість функціональних перетворень алгоритму $Al_i(Za_i)$ визначається на основі реалізації оберненої послідовності, що описується співвідношенням (4.1.).

Якщо $j(al_{ij})$ описує лінійне перетворення деякої змінної x_i, відтворити обернені процеси на рівні їх інтерпретації можна з точністю до визначення обернених функціональних перетворень. Це дає можливість повністю розсекретити конфіденційну величину x_i. Слід визначити наступні аспекти конфіденційності деякої величини x_i, що знаходиться в IS:

– конфіденційність значення величини x_i;
– конфіденційність інтерпретації деякої величини x_i;
– повна конфіденційність величини x_i.

Повна конфіденційність величини x_i означає, що невідомими є поточне значення величини x_i та невідомим є факт існування самої величини x_i. Очевидно, що повна конфіденційність x_i повинна бути відносною. Це означає, що існують умови або категорії користувачів, для яких факт існування x_i в середовищі IS є відомим. У протилежному випадку рівень конфіденційності переходить у деяку свою абстракцію, що визначається відсутністю будь-якої інформації про x_i, що рівнозначне тому, що x_i не існує взагалі. Очевидно, що для випадку IS такий рівень конфіденційності є не доцільний.

Конфіденційність інтерпретації x_i відповідає випадку, коли про існування x_i існує інформація, яка може мати різний рівень адекватності. Цей рівень адекватності визначається кількістю даних про параметри x_i, що характеризують відповідну компоненту. Такими даними не обов’язково є дані про x_i, що її характеризують не

залежно від природного або технічного оточення x_i. Відповідні дані можуть носити відносний характер, які описують взаємозв'язок з оточенням відповідних компонент x_i. Ці параметри або ці дані є найбільш поширеним способом опису інформації про деякі об'єкти, оскільки, в більшості випадків, довільна інформація про компоненти x_i може бути важливою, якщо остання стосується відображення зв'язків між x_i та їх оточенням. Такі дані описуються з допомогою текстових описів інтерпретації $j(x_i)$, які можуть мати різний рівень повноти, що формально описується співвідношенням:

$$Ad(x_i) = f[j_1(x_i) * j_2(x_i), \dots, j_m(x_i)]$$

де f – функція, яка описує взаємозв'язки між окремими фрагментами текстових описів x_i, а $j_i(x_i)$ – окремий фрагмент текстового опису $I(x_i)$. Рівень адекватності або величина значення $Ad(x_i)$ визначається досить складно. Тому необхідно впровадити наступне визначення.

Визначення 4.2. Інтерпретаційний опис x_i є повним для x_i, якщо будь-яке його розширення є надмірним.

Приведене визначення носить якісний характер і тому, залежно від розширення інформації про оточення x_i, величина і, відповідно, значення адекватності $Ad(x_i)$ може збільшуватися. Можна стверджувати, що будь-який опис x_i не може мати абсолютної повноти адекватності. Тому рівень $Ad(x_i)$ слід розглядати тільки як відносну величину.

У більшості випадків уявлення про конфіденційність деякої компоненти відповідає ситуації, коли така конфіденційність полягає в укриванні величини значення компоненти x_i, яка представляється деяким числом [131, 132]. У зв'язку з тим, що рівень конфіденційності, яким характеризується та чи інша величина x_i суттєво залежить від додаткових даних про компоненту x_i, наприклад про адресу розміщення x_i в IS або про рівень конфіденційності x_i, то дані, за якими звертаються задачі до IS, описуються в запитах у вигляді їх текстових описів, які мають різний рівень адекватності. Обґрунтованість такої форми звернення Za_i за даними типу $r_i^t(x_i)$ полягає в тому, що різні рівні конфіденційності потребують різну міру повноти інформації про дані, яка не може зводитися лише до інформації про числову величину відповідної компоненти x_i. Таким чином, рівень

конфіденційності інформації про x_i може визначатися мірою адекватності відомих описів $I(x_i) = \{j_1(x_i) * ... * j_m(x_i)\}$ реальної інтерпретації $I^*(x_i)$. Для того, щоб можна було говорити про управління рівнем конфіденційності даних, що знаходяться в IS, яка полягає у збільшенні чи зменшенні такого рівня, одним з можливих способів такого управління є збільшення або зменшення рівня адекватності $Ad_i(x_i)$, що описує інтерпретацію відповідних даних. Коли мова йде про зміну рівня конфіденційності x_i, очевидно, що цього можна досягнути шляхом збільшення рівня адекватності відповідного опису $Ad_i(x_i)$ розширення такого опису. Якщо мова йде про збільшення рівня конфіденційності деякої інформації про окрему компоненту, то мають місце наступні можливості. Якщо деяка компонента x_i мала рівень конфіденційності, який відповідав рівню адекватності $Ad_i(x_i) = \alpha$ і виникла необхідність зменшити рівень адекватності $Ad_i(x_i)$, з метою збільшення рівня конфіденційності відповідних даних, опис рівня адекватності, який представляє собою текстовий опис інтерпретації x_i необхідно модифікувати таким чином, щоб відповідна модифікація не призвела до семантичної суперечності, але звузила б реальний опис предметної області інтерпретації відповідної компоненти x_i. Оскільки IS приймається як об'єкт, який має найбільш повний, з точки зору адекватності, опис конфіденційних даних, то модифікація опису адекватності x_i з боку IS, може прийматися «як розширення», яке відповідає реальності, яку описує відповідна IS. Відомо, що фактичною реальністю, яку описує IS є предметна область інтерпретації W_i, яка може бути відомою користувачу, який співпрацює з IS. Тому виникає проблема зі створення розширення $j_{ij}^*(x_i)$, яке призвело б до зменшення рівня адекватності опису x_i або $Ad(x_j)$. Для розв'язання цієї проблеми необхідно в процесі аналізу враховувати щонайменше два аспекти:

– рівень співпраці довільних користувачів з предметною областю інтерпретації W_i;

– структурні та функціональні особливості W_i, що відображаються в інформаційних об'єктах, які входять до складу предметної області W_i;

– зв'язок між величиною збільшення рівня конфіденційності компоненти x_i та рівнем зменшення величини адекватності опису x_i або $Ad(x_i)$.

Крім управління рівнем конфіденційності даних, що знаходяться в IS, можна керувати рівнем безпеки $\beta(IS\&W_i)$ на основі використання різної глибини автентифікації задачі Za_i, яка звертається за конфіденційними даними. У цьому випадку, автентифікацію, можна розділити на автентифікацію початкову та функціональну. Початкова автентифікація Za_i полягає у перевірці даних до початку процесу розв'язання задачі.

Автентифікація функціональна полягає у перевірці процесу розв'язання задачі на різних етапах цього розв'язання. Початкова автентифікація реалізується у випадку, коли Za_i потребує даних з низьким рівнем адекватності та низьким рівнем конфіденційності. Автентифікація функціональна проводиться у випадках, коли задача звертається за даними високого рівня конфіденційності. Вона полягає у використанні для фрагментів $Al_i(Za_i)$ внутрішніх алгоритмів перетворення конфіденційних даних, що реалізуються не в рамках задачі, а в рамках системи SNP. У цьому випадку автентифікація полягає у перевірці рівня узгодженості вихідних даних, що отримані у результаті використання внутрішніх алгоритмів, з даними, що отримані в результаті використання фрагментів $al_{ij} \in Al_i(Za_i)$, які використовують в якості вхідних даних результатів роботи $Az[r_i(x_i)]$.

Крім приведених вище характеристик даних та інших компонент системи надання повноважень, для отримання доступу до тих чи інших параметрів, необхідно системі SNP надати характеристики задачі Za_i. Першою з таких характеристик є величина семантичної суперечності задачі:

$$\sigma^s\{C_i(Za_i)\&[\,Al_i(Za_i)]\&Dw_i(Za)\}.$$

У цьому випадку мета $C_i(Za_i)$ описується у вигляді деякої структури, а вхідні дані Dw_i описуються областями визначення відповідних вхідних параметрів, що використовується в $C_i(Za)$ та $Al(Za_i)$. Очевидно, що Dw_i також представляють собою текстові описи їх інтерпретації, на основі яких відповідні Dw_i вибираються з IS, якщо доступ до даних система SNP надає. Якщо $\sigma^s\{C_i\&(Al)\&Dw_i\}$ є суперечна, то SNP відмовляє задач Za_i у доступі до даних.

Кожна задача, що використовує конфіденційні дані, має свій власний параметр конфіденційності $P(Za_i) = P[M(Za_i), r(Za_i)]$. У цьому випадку, система SNP перевіряє чи $r_i^{et}(x_i) \geq max\ p^r(Za_i) \pm \delta p_i(Za_i)$.

Оскільки r_i^{et} визначає інтервал конфіденційності або її рівень, то перевіряється приведена нерівність. Аналогічно здійснюється перевірка в частині, що стосується рівня конфіденційності задачі, який повинен також відповідати заданій величині $\mu(x_i)$.

Значимість задачі $\aleph_i(Za_i)$ представляє собою параметр аналогічний параметру $\aleph_i(x_i)$. Тому він також перевіряється шляхом реалізації порогового контрою різниці між $\aleph_i(x_i \in Za_i)$ та $\aleph_i(Za_i)$.

Актуальність задачі $Ak(Za_i)$ визначається певними критеріями, що відображають еволюційність змін в W_i у результаті розв'язання задачі Za_i [125]. Такі критерії формуються на основі аналізу W_i і описуються як критерії змін, що можуть відбуватися в W_i у наслідок дії на W_i результатів розв'язання окремих задач. Оскільки перед розв'язанням задачі система SNP має можливість аналізувати лише опис мети задачі $C_i(Za)$, визначення величини рівня актуальності $Ak(Za_i)$ може здійснюватися лише з точністю, яку може забезпечити опис $C_i(Za_i)$. Тому рівень $Ak(Za_i)$, визначений на початковому етапі, може виявитися дещо відмінним від реального ефекту впливу розв'язання Za_i на W_i. У зв'язку з цим система IS аналізує дані про реальний вплив результатів розв'язання задачі на Za_i і зберігає відповідні дані у наступній формі. Для кожної задачі Za_i, що звертається в IS за конфіденційними даними, система SNP формує профіль задачі, який містить всі параметри, які мають до задачі відношення, включаючи параметри даних та інформаційні параметри і який позначається $Prf(Za_i)$. Якщо окремі параметри для цієї задачі змінилися після розв'язання останньої, відповідні параметри корегуються у профілі задачі $Prf(Za_i)$. Прикладом таких параметрів, які можуть змінюватися, може бути не лише параметр $Ak(Za_i)$, а і параметр, що змінюється обов'язково $\aleph(Za_i)$, що виникає з його визначення. Навіть параметр конфіденційності може

змінюватися у відповідності з положенням, згідно з яким рівень конфіденційності може зменшуватися з ростом параметра $\aleph_i(x_i)$.

До інформаційних параметрів, що характеризують задачу [4], відносяться:

– параметр доповнення P_c;
– параметр повторення P_p;
– параметр дублювання P_d.

Приведенні параметри встановлюються в процесі аналізу задачі, який проводить SNP у випадку, коли Za_i звернулася до SNP за обслуговуванням. Параметр P_c визначає розбіжність між $C_i(Za_i)$ та компонентами задачі $Al(Za)$ та $Dw(Za_i)$. Цей параметр визначається у випадку, коли між $C_i(Za_i)$ і іншими компонентами Za_i виникає суперечність. Ця суперечність, для даного випадку, є дещо специфічна на відміну від класичного уявлення про суперечність. Відрізняються вони тим, що суперечність виникає у випадку, коли $Dw_i(Za_i)$ чи $Al(Za_i)$ ілюструють факт існування недостатньої визначеності $C_i(Za_i)$ по відношенню до $Dw_i(Za_i)$ та $Al(Za_i)$. Наприклад, в Dw_i існують дані, що використовуються в $Al(Za_i)$, а в $C_i(Za_i)$ відсутня будь-яка інформація про результати розв'язання Za_i, які були б пов'язані з відповідними фрагментами Dw_i і Al_i. Параметр P_p означає повторення задачі, яка уже розв'язувалася. Параметр P_d означає дублювання задачі, яка уже розв'язувалася для W_i.

Після співпраці системи IS з задачами та наданню задачам конфіденційних даних, виникає необхідність визначення, чи не змінився суттєво рівень безпеки системи IS вцілому. Для цього необхідно визначити період співпраці з задачами та умови, за яких така перевірка повинна реалізовуватися. Передача конфіденційних даних, для їх використання задачами є тим фактором, який може суттєво впливати на рівень безпеки системи IS. Оскільки рівень безпеки системи IS є оцінкою інтегральною, яка залежить від цілого ряду факторів, насамперед необхідно визначити поточні значення оцінок цих факторів. Першим з таких факторів є рівень конфіденційності та частота використання конфіденційних даних. Наступним фактором є рівень прогресивності змін, до яких призвело використання результатів

розв’язання задач. Третім фактором є кількість задач, яким система відмовила у наданні повноважень на використання конфіденційних даних та ряд інших факторів, які носять більш детальний характер.

Розглянемо параметр конфіденційності і розглянемо функцію, яка пов’язує параметр r_i^{it} з $\beta(IS)$. Кількісне співвідношення на деякому загальному рівні буде виглядати наступним способом. Приймемо, що небезпека β деякої системи IS визначається кількістю рівнів конфіденційності даних, які в IS знаходяться. Безпека чи небезпека по відношенню до самої IS, як деякої інформаційної системи немає сенсу. Небезпека чи необхідний рівень безпеки IS повинен оцінюватися тими втратами у середовищі W_i, до яких може призводити використання даних з IS для розв’язання задач Za_i, які є несанкціонованими. Такі задачі будемо позначати Za_i^n. Система захисту, яка реалізується в IS, повинна розпізнавати серед всіх можливих задач Za_i несанкціоновані задачі Za_i^n. Несанкціоновані задачі, з точки зору використання результатів їх розв’язання в W_i, є такі задачі, використання яких призводить до зменшення функціональних можливостей W_i відносно до встановленої їх кількості, при формуванні або проектуванні об’єкту, який становить предметну область інтерпретації даних з IS. Допустимі різні варіанти визначення негативних змін в W_i, але приведений спосіб визначення негативних змін будемо вважати достатньо універсальним. Тому рівень негативних змін в W_i, які відбуваються в результаті реалізації Za_i^n, будемо вимірювати в процентах. Виходячи з того, що використання конфіденційних даних з IS може призводити до суттєвих негативних змін в W_i, приймаємо, що $r_i^{et}(x_i)$ визначається деякою безрозмірною величиною, яка відповідає проценту ушкоджень, до яких може призвести Za_i^n, що використовує $r_i^{et}(x_i)$. Таким способом визначення необхідного рівня конфіденційності $x_i \in IS$ дозволяє виключити можливість використання суб’єктивних факторів при визначенні рівня конфіденційності даних в деякій IS. При такій інтерпретації необхідного рівня конфіденційності даних $x_i \in IS$, можна прийняти, що зниження рівня конфіденційності x_i призводить до зниження рівня безпеки $\beta(IS)$ в цілому.

Виходячи з викладеного вище, можна зіставляти рівень безпеки $\beta(IS)$ із здатністю засобів захисту IS, у даному випадку системи SNP, розпізнавати серед всіх можливих задач Za_i, задачі, що є несанкціонованими або задачі Za_i^n. Система SNP реалізує перевірку параметрів даних, за якими звертається задача, та перевірку значень параметрів самої задачі, що звернулася за отриманням даних до IS і, відповідно, SNP. У даному випадку не розглядається ситуація, коли несанкціонована задача звертається за даними, які не є конфіденційними. У цьому випадку приймається, що несанкціоновану задачу може пропонувати тільки несанкціонований користувач. Кожний користувач, що звертається до системи, автентифікуються системою захисту доступу.

Розглянемо процеси, які реалізує система захисту або система безпеки (SB) в процесі аналізу параметрів даних задач, які реалізує SNP з точки зору їх впливу на величину безпеки IS.

У роботі розглядаються наступні три ключові рівні безпеки, які мають наступну інтерпретацію.

Перший випадок або перший виділений рівень конфіденційності відповідає ситуації, коли дані не передаються задачі Za_i, а їх перетворення реалізується алгоритмами Az_i, що декларуються як такі, що реалізують допустимі перетворення над $r_i^{et}(x_i)$ з точки зору втрат, до яких можуть призвести їх перетворення іншими алгоритмами. Внутрішні алгоритми $Az_i \in SNP$ вибираються на основі опису фрагментів мети $C_{ij} \in C_i(Za_i)$ для досягнення якої використовувались дані $r_i^{1t}(x_i)$. Крім відповідного фрагмента $c_{ij} \in C_i$ для вибору $Az_i[r_i^{1t}(x_i)]$ використовується схема фрагменту алгоритму розв'язання задачі, який безпосередньо призначений для перетворень даних типу $r_i^{1t}(x_i)$. Це, з одного боку означає, що на основі інтерпретації конфіденційних даних, що формуються на основі W_i, вибирається Az_i, яка є найбільш подібною до відповідного $al_i \in Al_i(Za_i)$, а з другого вона реалізує перетворення, які є допустимими для $r_i^{1t}(x_i)$. Завдяки цьому задача не зможе використати дані x_i таким чином, щоб вони призвели до виникнення аномалій в W_i.

Якщо $C_{ij} \in C_i$ відрізняється від $Az_i(x_i) \to c_{ij}(Az_i)$, це означає, що задача має ознаки несанкціонованності.

Другий виділений рівень конфіденційності відповідає ситуації, коли для $r_i^{2t}(x_i)$ в SNP не існує Az_i, які могли б реалізувати перетворення x_i, таким чином, щоб $Az_i r_i^{2t}(x_i) = C_{ij}(x_i)[al_i \in Al_i(Za) \to C_{ij}^*]\&[C_{ij}^*(x_j) \neq C_{ij}^*(al_{ij})]$. Це означає, що неможливо до SNP додати необхідний Az_i та звести ситуацію до першого виділеного рівня конфіденційності. Це означає, що для $r_i^{2t}(x_i)$ існує тільки можливість реалізації такого перетворення, яке на виході дає дискретний результат, який формується на основі текстового опису інтерпретації $j[r_i^{2t}(x_i)]$ та інтерпретації фрагменту алгоритму $al_i \in Al_i(Za_i)$, який запропонований у задачі і стосується переважно конфіденційних даних. Наприклад, якщо в результаті роботи $al_{ij}(r_i^{2t}(x_i))$ передбачалося отримати деякий результат $c_{ij}(al_{ij})$, то $c_{ij}(r_i^{2t}(x_i))$ буде представляти собою результат у формі дискретної величини, що стосується предметної області інтерпретації відповідної мети. Алгоритми, які використовуються у таких цілях, формуються виходячи з опису інтерпретації та особливостей інтерпретації конфіденційних даних, що відносяться до другого вибраного рівня конфіденційності. Це означає, що існують дані, які можна перетворювати лише визначеними способами, а в результаті отримати дискретний результат. У роботі такі алгоритми називаються декларативними Ad_i.

На третьому вибраному рівні конфіденційності $r_i^{3t}(x_i)$ зберігаються дані, які на рівні сформованих задач використовувати безпосередньо неможливо. Це визначається на основі опису текстової інтерпретації цих даних. У цьому випадку SNP реалізує або формує доповнення, або модифікує мету задачі та відповідних даних. Така модифікація не повинна суперечити умові задачі та її параметрам. Результат модифікації $r_i^{3t}(x_i)$ по суті, змінює поточне значення $r_i^{3t}(x_i)$, та модифікує інтерпретацію відповідних даних. У модифікованій формі відповідні дані можуть передаватися до задачі Za_i для використання. Виходячи з приведеного, можна було б стверджувати, що такого типу дані $r_i^{3t}(x_i)$ немає сенсу взагалі розміщати в IS. Але дані такого типу існують в W_i і відносяться до класу критичних

даних x_i^k. Наприклад, якщо параметр x_i^* в IS можна використовувати як критичний у відповідних перетвореннях, то це має місце тоді, коли нам необхідно моделювати деякі критичні процеси. Тому можна стверджувати, що конфіденційні дані, які відносяться до вибраних даних третього типу можна безпосередньо використовувати тільки у задачах моделювання тих чи інших процесів в W_i. Задачі Za_i про які йде мова, представляють собою засоби перетворень, результати яких використовуються безпосередньо в W_i. Якщо W_i має параметри, що характеризують критичні стани в W_i, то їх використання для перетворень можна використовувати тільки для моделювання відповідних фрагментів в W_i. На основі такого моделювання формуються дані, які можна використовувати в задачах, що орієнтовані на впровадження змін у відповідному середовищі. Необхідність в активізації такого моделювання визначається появою задач Za_i, які потребують дані, що відносяться до третього виділеного рівня конфіденційності. Очевидно, що при введенні таких даних в IS, повинні вводитися в IS засоби моделювання процесів в W_i, які ґрунтуються на використанні цих даних.

Ця ситуація означає наступне. Якщо виникає задача, яка орієнтована на впровадження змін, пов'язаних з критичними параметрами, то насамперед необхідно провести моделювання цих змін в W_i, і тільки за результатами моделювання приймаються рішення з активізації тих чи інших змін в W_i. У зв'язку з цим, розглянемо деякі загальні характеристики IS та сформулюємо відповідні умови, що враховуються, при використанні розроблених методів організації системи SNP.

Приймемо наступний розподіл параметрів, що характеризують систему в цілому:

– параметри та фактори, що характеризують систему з точки зору її надійності;
– параметри та фактори, що характеризують безпеку системи.

Надійність системи, як і будь-якого штучного об'єкту, у відповідності з загально прийнятими уявленнями, характеризує здатність системи реалізовувати процеси функціонування, які передбачені технічним завданням на систему [126, 127]. Тому для забезпечення надійності в IS повинні розв'язуватися наступні задачі:

– контроль доступу користувачів до системи;
– надання користувачу тих чи інших даних, що знаходяться в системі;
– управління повноваженнями до способу використання отриманих даних.

Безпека системи типу IS характеризує здатність виконувати ряд додаткових функцій, що пов'язані з виявленням та протидією факторам, орієнтованими на реалізацію протидії процесу функціонування і спеціально активізуються для, унеможливлення або спотворення процесів функціонування системи, що передбачені відповідними вимогами до неї [11, 128]. Безпека системи відображає здатність останньої протидіяти впливу на неї негативних факторів технічного або штучного характеру.

Для більш чіткого відокремлення обставини, що стосуються надійності IS та безпеки IS, введемо наступні умови.

Умова 4.1. Всі фактори штучного походження, що негативно впливають на процес функціонування IS, приймаються як фактори, що загрожують безпеці системи.

Умова 4.2. Якщо система містить дані або інші елементи використання яких може призвести до негативних наслідків в предметній області інтерпретації W_i, яку обслуговує система, остання повинна включати в себе засоби її захисту.

Умова 4.3. Якщо на етапі проектування системи передбачається можливість виникнення негативних факторів невідомої природи, що характерно для систем, які функціонують порівняно довгий час, то в рамках системи передбачаються компоненти забезпечення можливості системи протидіяти таким факторам, тобто володіти здатністю розпізнавати невідомі негативні фактори та протидіяти їх впливу на систему.

Умова 4.4. Якщо в систему можна увести змінені дані, використання яких може призвести до наслідків, що не передбачалися функціональними вимогами до системи, то система повинна контролювати вхідні дані.

З наведених вище умов випливає, що під безпекою системи IS (на відміну від її надійності), вважається можливість системи безпеки протидіяти негативному впливу, який може виникнути при використанні результатів розв'язання задач.

4.3 Загальна організація роботи системи управління наданням повноважень та реалізація відповідних алгоритмів

Загальна організація роботи системи безпеки IS, яка включає систему надання повноважень, повинна охоплювати всі складові, що входять в систему і забезпечують той чи інший рівень безпеки. До функціональних складових відносять наступні:

- оцінка поточного рівня безпеки IS;
- управління рівнем конфіденційності даних;
- рівень забезпечення задач даними;
- визначення кількості несанкціонованих задач;
- зв'язок системи IS з безпекою W_i;
- моніторинг оцінки безпеки системи;
- управління безпекою та протидія її порушенням.

Оцінка поточного рівня безпеки є процесом, який враховує цілий ряд поточних значень параметрів, що характеризують безпеку та враховують ряд факторів, що впливають на її величину. До таких параметрів та факторів відносяться:

- рівень конфіденційності даних та інші параметри, що характеризують дані;
- параметри, що характеризують безпеку доступу до системи окремих користувачів;
- параметри, що характеризують процеси автентифікації задач, що звертаються за конфіденційними даними;
- характеристики факторів, дія яких призводить до порушення рівня безпеки IS;
- характеристика процесів прогнозування поточного рівня безпеки системи.

Безпека будь-якої інформаційної системи передбачає забезпечення наступних можливостей:

- можливості функціонувати у відповідності з вимогами, що сформульовані до системи;

– забезпечення необхідної величини рівня конфіденційності даних чи процесів, якщо їх використання передбачене відповідною системою;

– забезпечення прогресивності змін, якщо останні передбачаються системою.

Функціонування інформаційних систем, що представляють собою бази даних BD, орієнтованих на обслуговування тих чи інших предметних областей інтерпретації, порівняно з IS, є досить обмежене і стосується в основному процесів контролю доступу до даних та процесів управління параметрами даних, якщо це обумовлено статусом відповідних даних. До процесів, що реалізуються в системах типу IS, відносяться допоміжні процеси, які реалізують функції оцінки різних параметрів системи з метою надання відповідної інформації про систему користувачам.

У роботі розроблено ряд алгоритмів, що реалізують результати досліджень.

На рисунку 4.1 приведена блок-схема процесу аналізу, який реалізує SNP. Використовуємо наступні позначення:

– OD – перевірка, чи присутній текстовий опис даних;

– WD – визначення адреси даних;

– DT – визначення, чи дані є конфіденційними;

– VTZ – визначення рівня конфіденційності задачі;

– ZP – визначення, чи рівень конфіденційності задачі є більший або рівний рівню конфіденційності даних;

– NSN – негативний вихід з системи надання повноважень;

– WPV – визначення параметра значимості моделі даних;

– ZD – перевірка, чи величина значимості моделі даних є допустимою;

– VPA – визначення параметра актуальності моделі даних;

– AD – перевірка, чи значення параметра актуальності моделі даних є допустимим;

– VPS – визначення суперечності задачі;

– SZ – перевірка, чи величина суперечності задачі є допустимою;

– VAZ – визначення актуальності задачі;

– AZ – перевірка, чи величина актуальності задачі є допустимою;

– VZZ – визначення значимості задачі;

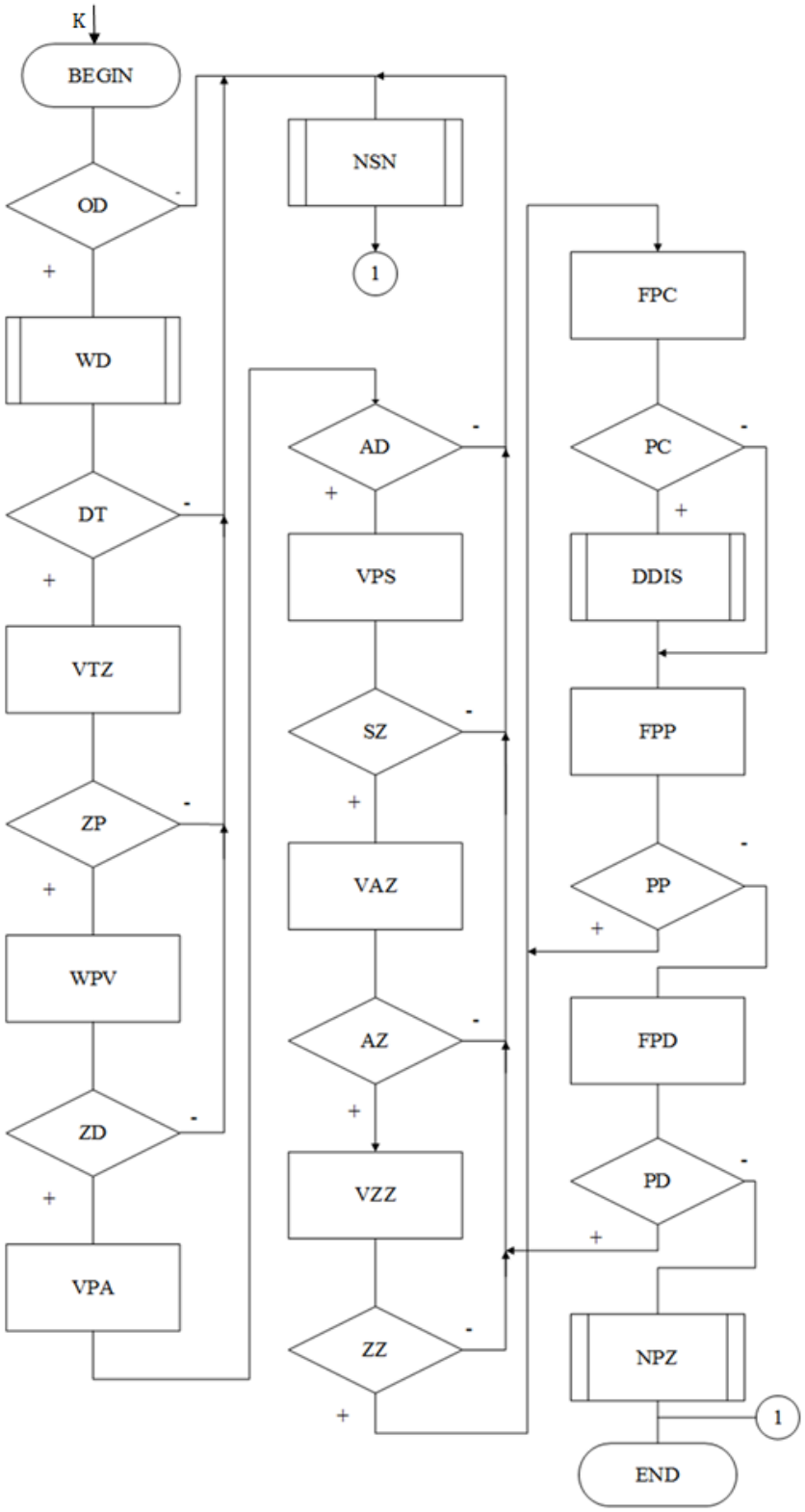

Рис. 4.1. Блок-схема процесу надання повноважень

– PC – перевірка, чи повинна задача доповнити IS новними значеннями параметрів;

– ZZ – перевірка, чи величина значимості задачі є допустимою;

– FPC – формування параметру доповнення даними системи IS;

– FPP – формування параметру повторення задачі;

– DIS – доповнення інформаційної системи новими параметрами;

– PP – перевірка, чи задача не повторюється;

– FPD – формування параметру дублювання задачі;

– PD – перевірка, чи має місце дублювання задачі;

– NPZ – надання повноважень задачі на використання даних, за якими задача звернулася до системи IS.

На рис. 4.2. приведено блок-схему загальної організації функціонування системи IS. Використовуються наступні позначення:

– K – користувач;

– IK – ідентифікація користувача;

– IU – перевірка, чи ідентифікація користувача успішна;

– VK – відмова користувачу;

– TOD – текстовий опис інтерпретації даних;

– MT – визначення, чи є запит на конфіденційні дані;

– NO – перевірка, чи є обмеження на використання даних;

– NDK – надання даних користувачу;

– BI – блокування заборонених перетворень даних в системі IS;

– PZR – позитивне завершення роботи системи;

– RMT – визначення рівня конфіденційності чергових вхідних даних, щодо яких здійснюється запит;

– $1T$ – перевірка, чи дані відносяться до першого рівня конфіденційності;

– $VRAT$ – вибір і реалізація відповідного внутрішнього алгоритму перетворення конфіденційних даних;

– TD – перевірка, чи є в задачі необхідність використання конфіденційних даних;

– RTZ – продовження розв’язання задачі з даними, що не є конфіденційними;

– CZ – перевірка, чи отримана мета відображає мету, що описана в задачі;

– $2T$ – перевірка, чи дані відносяться до другого рівня конфіденційності;

– $VRAD$ – визначення і реалізація відповідних алгоритмів, що використовують дані другого рівня конфіденційності;

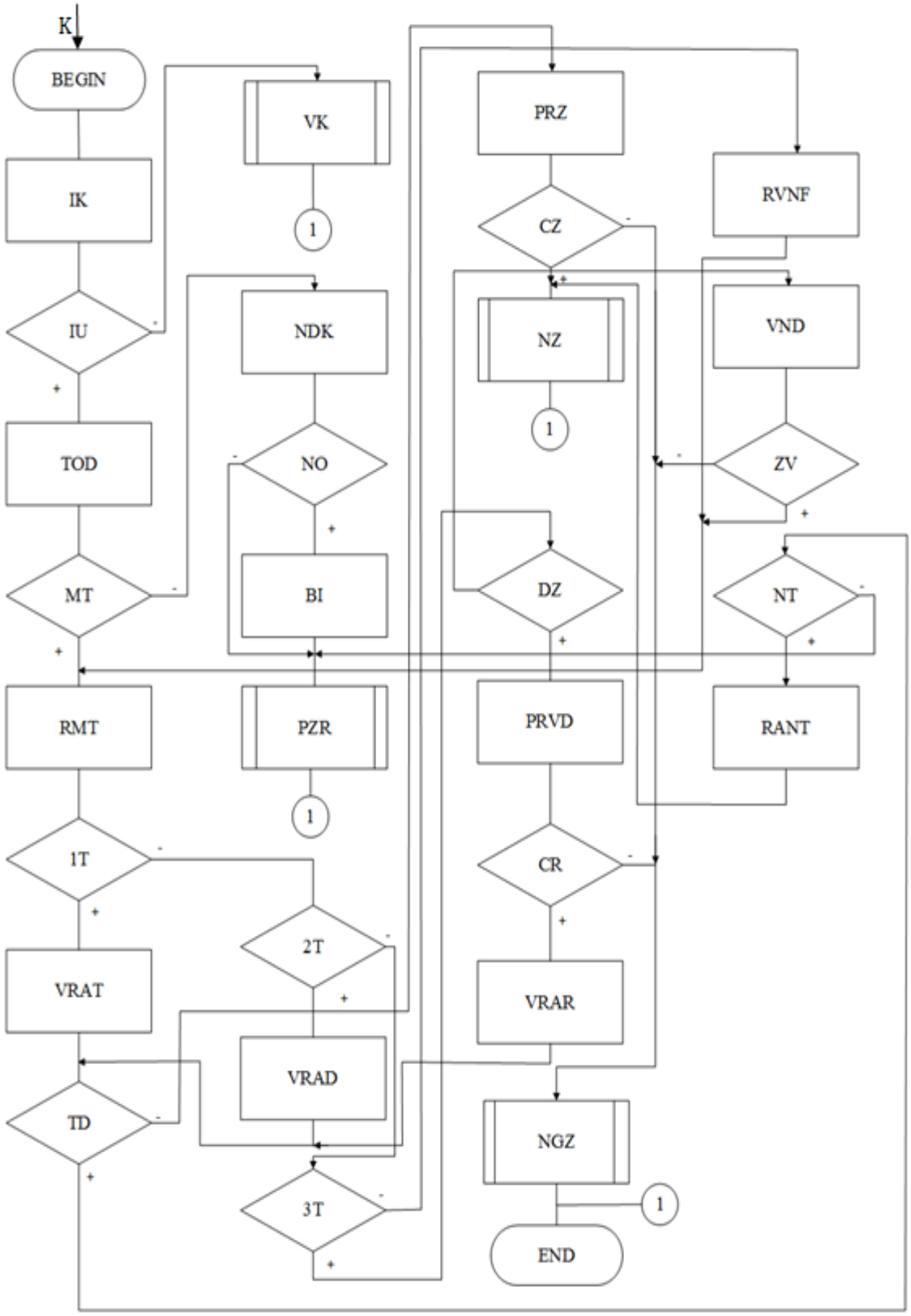

Рис. 4.2. Блок – схема загальної організації функціонування системи IS.

– $3T$ – визначення, чи дані відносяться до третього рівня конфіденційності, які потребує задача;

– PRZ – прийняття рішень про допустимість, чи не допустимість використання даних третього рівня конфіденційності;

– DZ – перевірка, чи задача може використовувати дані третього рівня конфіденційності;

– $PRVD$ – прийняття рішень про спосіб використання конфіденційних даних третього рівня;

– CR – перевірка, чи мета задачі не суперечить можливому розв'язання задачі;

– $VRAR$ – визначення і реалізація алгоритму, що відповідає прийнятому рішенню;

– $RVNF$ – реалізація відповідного фрагмента алгоритму задачі, що використовує не конфіденційні дані;

– NGZ – негативне завершення розв'язання задачі;

– VND – відмова у використанні даних третього рівня конфіденційності поточною задачею;

– ZV – перевірка, чи задача змінила вимоги до даних;

– NT – перевірка, чи використання конфіденційних даних є необхідне даній задачі;

– $RANT$ – реалізація фрагменту алгоритму, що не потребує конфіденційних даних;

– NZ – нормальне завершення роботи.

Управління рівнем безпеки є однією з ключових функцій системи типу IS з наступних причин.

Рівень безпеки системи, якщо остання є активною протягом різних інтервалів її функціонування, змінюється з різних причин, прикладами яких можуть бути:

– природні зміни рівня безпеки;

– функціональні зміни рівня безпеки;

– декларативні зміни рівня безпеки;

– непередбачувані зміни рівня безпеки;

– обумовлені зміни рівня безпеки.

Природні зміни рівня безпеки обумовлюються факторами, що характеризують особливості процесу функціонування системи та основних її компонент. Ці зміни є відомими, а також відомі залежності між причинами зміни безпеки та рівнем безпеки. У багатьох випадках об’єднання причин зміни рівня безпеки реалізується на основі припущення, що кожна з таких компонент є незалежною і для опису інтегральної оцінки, вони додаються і за необхідності, усереднюються [129, 130]. Прикладом таких природних змін може бути зміна рівня конфіденційності даних $r_i^t(x_i)$, який змінюється з часом.

Ураховуючи викладене вище, використання дворівневої моделі доступу до даних дозволяє створити програмне забезпечення, яке за певних умов може отримати доступ до інформації більш високого рівня доступу, не розголошуючи її змісту. Розглянемо прикладну задачу, не розкриваючи повністю предметну область інтерпретації, а обмежившись лише критичними умовами її реалізації. Задано три суміжні області *A, B, C***.** Причому області *A* і *C* не мають спільних кордонів і шлях з *A* в *C* пролягає через *B*. У області *B* розташовано деякі об'єкти, інформація про які є конфіденційною. Нам необхідно провести об'єкт з області *A* в область *C*. При цьому не розголошуючи конфіденційної інформації з області *B*. Класична модель доступу вирішує цю проблему за рахунок обходу області *B* межею. Використовуючи дворівневу модель доступу до даних, можна побудувати критерій не розголошення конфіденційної інформації. Наприклад, дозволити рух об'єкта в області *B* та, аналізуючи траєкторію його руху, з метою не допущення його попадання у деяку область контакту об'єктів з області *B*. За рахунок цього буде відбуватися скорочення проходження шляху об'єкта. Слід зауважити, що існує деяка мінімальна відстань, менше якої скоротити шлях неможливо. Проведемо серії експериментів, генеруючи в області *B* чотири об'єкти, випадковим чином дотримуючись рівномірного розподілу (завдання контролю об'єкта, забороненої території і території обмеженого доступу), для об'єкта з області *A* будується гарантований обхідний маршрут і будується маршрут проходження через область *B* з деякою точністю *H*. Критерієм не розголошення встановимо не допущення наближення об'єкта з області *A* до

об'єктів з області *B* на відстань *D*. Алгоритм пошуку шляху у таких умовах працює не отримуючи інформації про розташування об’єктів області *B*, що відповідає нашим вимогам з конфіденційності. Результатом експерименту буде розрахунок довжини скороченого шляху у частках від максимального (обхідного) шляху.

Для реалізації програмного забезпечення було обрано мову програмування Python 2.7. Загальна назва розробленого програмного пакета «Security Visualizer». Даний пакет складається з наступних програмних модулів: «matrixmodel.exe» – меню, яке дозволяє обрати параметри запуску для «visualizer.exe»; «visualizer.exe» – програма, яка відображає карту з точками, до яких має доступ користувач. Вона приймає від «matrixmodel.exe» або командного рядка два аргументи - рівень і колір доступу користувача та читає точки з файлів «red.csv», «green.csv», «blue.csv», «yellow.csv». Зазначені файли необхідні для вивчення і демонстрації матричної моделі доступу. Друга група файлів, яка входить до програмного пакету «Security Visualizer» реалізує модель пошуку шляху. Це «pathfindermodel.exe» – меню, яке дозволяє вибрати параметри запуску для pathfinder.exe; «pathfinder.exe» – програма, яка знаходить на карті між двома заданими точками наближено найкоротший маршрут, який обминає кожну з чотирьох точок, які випадково згенеровано у просторі між початковою і кінцевою точками. Відображає усі точки, знайдений маршрут і окремий обхідний маршрут, який складається з двох відрізків і гарантовано обминає згенеровані точки. Програма «pathfinder.exe» приймає від «pathfindermodel.exe» або командного рядка два обов’язкові аргументи: радіус наближення (мінімальна відстань, на яку може наблизитися маршрут до точки) і точність розрахунку маршруту. Також у режимі командного рядка може приймати третій аргумент – кількість експериментів. Зазначена програма здійснює експеримент (генерація набору з чотирьох точок і пошук найкоротшого маршруту). Для кожного експерименту запам'ятовується довжина знайденого маршруту як відсоток від довжини обхідного маршруту. Ця інформація записуються у файл «result.csv». Початкова і кінцева точки читаються з файлів «start.csv» і «end.csv» відповідно. Всі програмні модулі використовують вхідні дані з папки «data». Алгоритм пошуку засновано на відомому алгоритмі Лі з метою здійснення

виявлення найкоротшого шляху на основі графів з ребрами одиничної довжини. Цей алгоритм належить до групи алгоритмів пошуку в ширину та призначений для визначення найбільш короткого шляху. Його цільове призначення є знаходження довжини.

Таким чином, для проведення експерименту необхідно запустити «pathfindermodel.exe». У меню (рис. 4.3) задати параметри моделювання і відкрити карту (рис. 4.4).

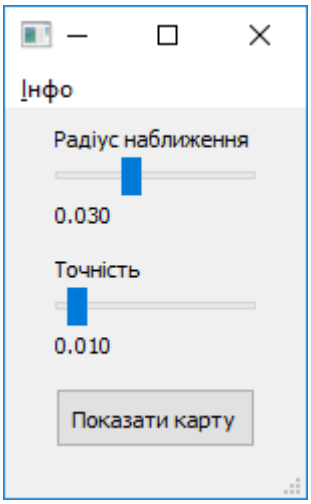

Рис 4.3. Меню вибору параметрів

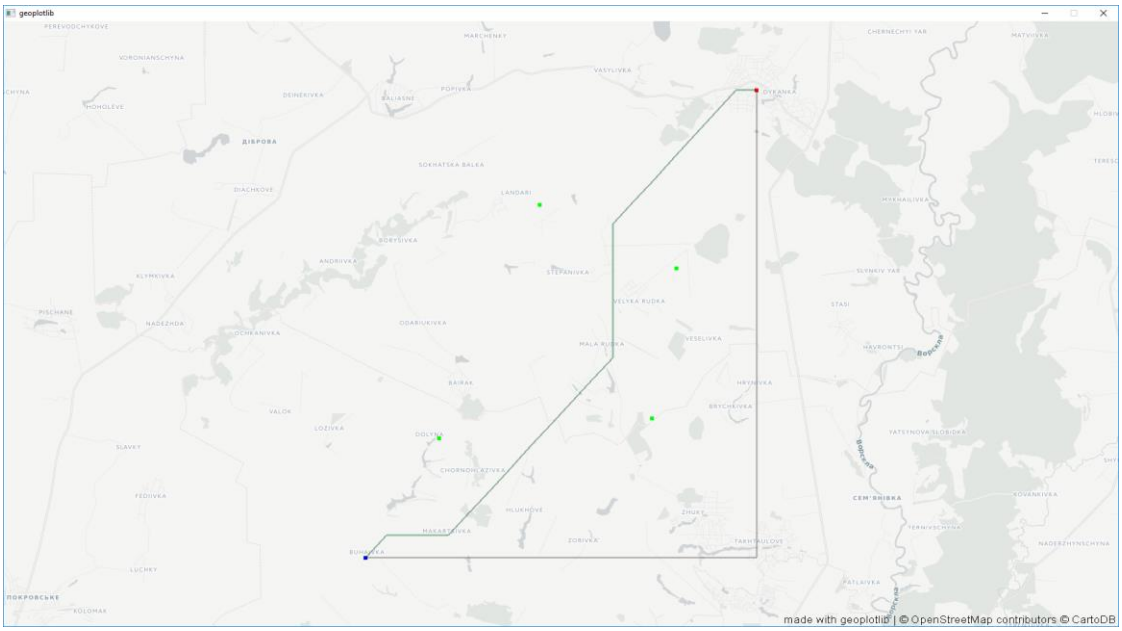

Рис 4.4. Результати одиничного розрахунку

На карті видно обхідний маршрут (горизонтальна і вертикальна прямі), синя і червона точки – початок і кінець маршруту, зелені точки – доступ, до яких

заборонено, і ламана крива лінія показує маршрут, який розроблено з використанням дворівневої моделі доступу до даних.

Для оцінки користі від застосування дворівневої моделі доступу до даних у даній прикладній задачі проведемо 1000 експериментів, результати яких наведено на рисунку 4.5. По осі Y показано кількість точок, що потрапляють в інтервал, який аналізується; по осі X – частка від максимального шляху. Математичне сподівання

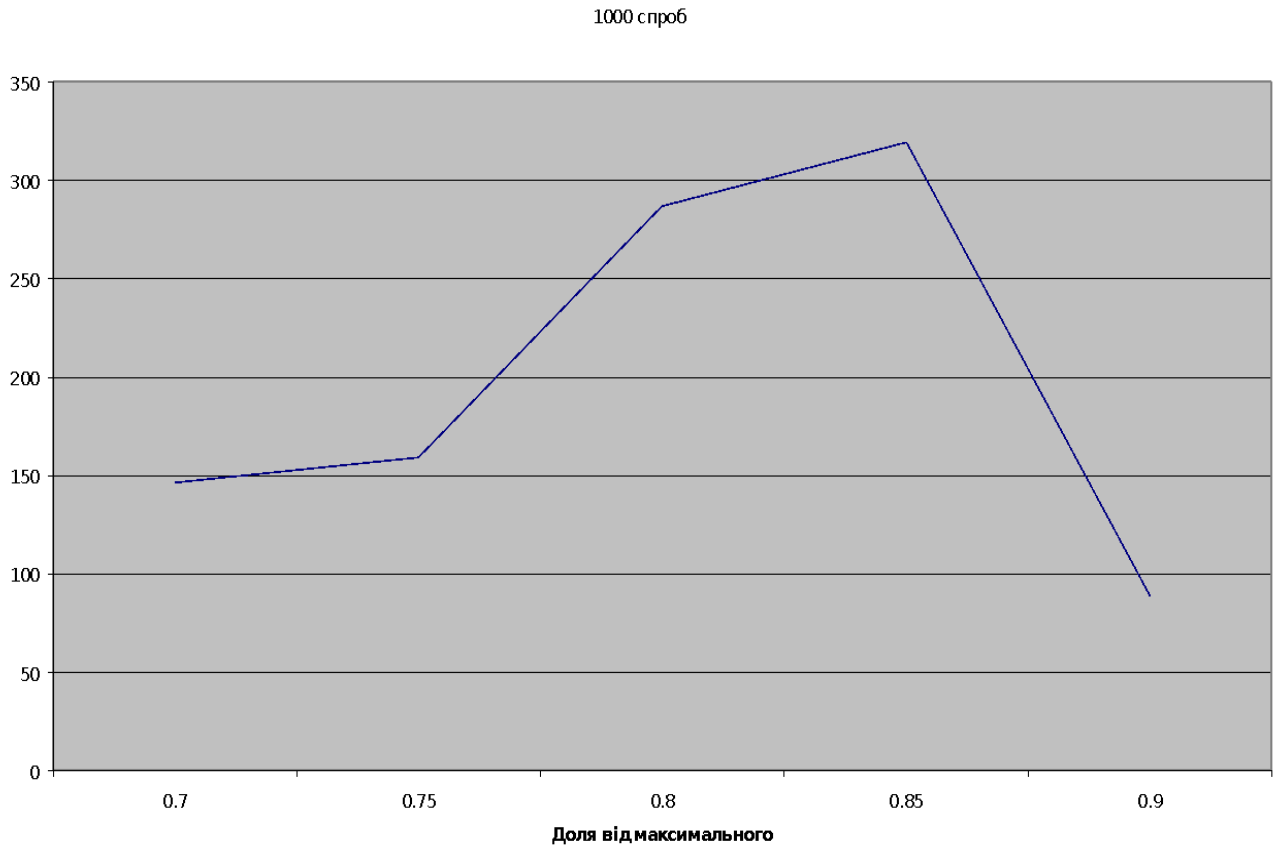

Рис.4.5. Результати тисячі експериментів

частки шляху становить 0,8025. Тобто середній виграш від застосування дворівневої моделі доступу до даних, при 1000 експериментах становить 19,75% від максимального шляху.

Характер кривої нагадує нормальний розподіл. Для уточнення побудуємо поверхню, яка показує результати більшого числа експериментів. У таблиці 4.1.наведено розподіл кількості результатів при фіксованих *D* і *H* для різного числа експериментів.

Таблиця 4.1

Розподіл кількості результатів для різного числа експериментів

Радіус наближення D	Точність розра-хунку H	Кількість точок в інтервалі X±0.025					Число експериментів
		0.7	0.75	0.8	0.85	0.9	
0.03	0.01	146	159	287	319	89	1000
0.03	0.01	242	357	561	653	187	2000
0.03	0.01	345	510	842	980	323	3000
0.03	0.01	461	670	1120	1319	430	4000
0.03	0.01	610	925	1300	1655	510	5000
0.03	0.01	745	1075	1685	1865	630	6000
0.03	0.01	831	1235	1959	2245	730	7000
0.03	0.01	971	1435	2175	2509	910	8000
0.03	0.01	1123	1610	2400	2797	1070	9000
0.03	0.01	1250	1800	2720	3133	1097	10000

На рисунку 4.6 приведено графічні результати проведених експериментів при зростанні їх числа.

Аналізуючи отриману поверхню видно, що із збільшенням кількості

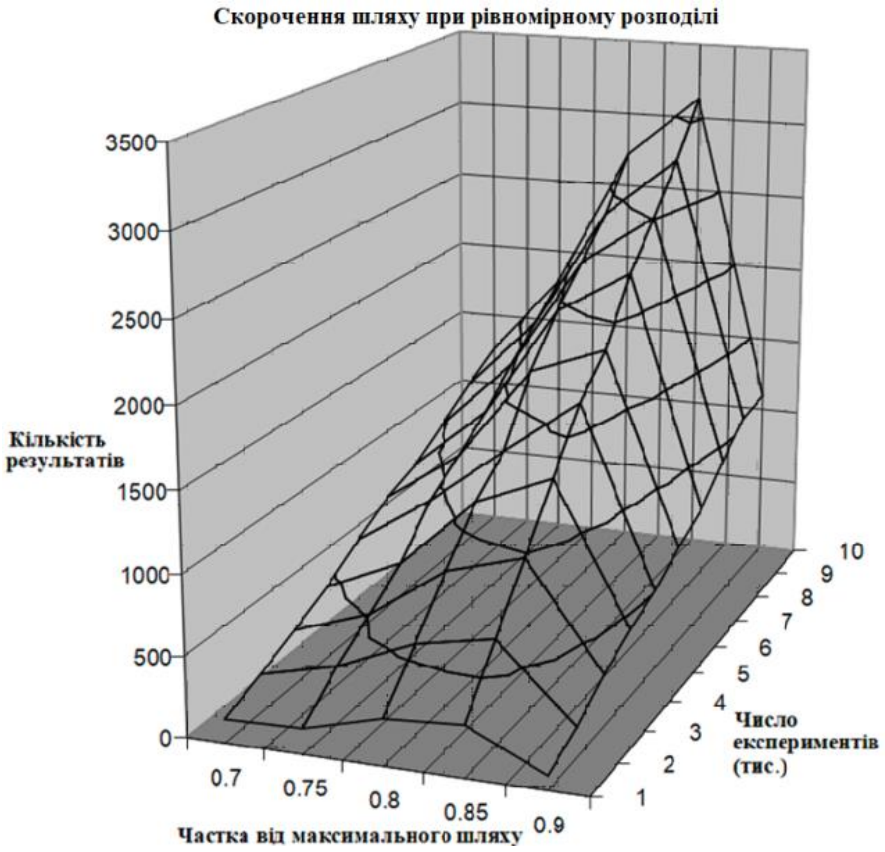

Рис. 4.6. Результати експериментальних досліджень

проведених експериментів форма кривої наближається до класичної для

нормального розподілу. Математичне сподівання частки шляху становить 0,8113 тобто середній виграш від застосування дворівневої моделі при 10000 експериментах становить майже 19% від максимального шляху.

Висновки до розділу 4

У четвертому розділі розв’язуються задачі реалізації алгоритмів надання повноважень, що ґрунтуються на досліджених методах розв’язання задач надання цих повноважень.

Основні зміни у предметній області інтерпретації, до яких призводить використання у предметній області інтерпретації результатів розв’язання прикладних задач, повинні бути прогресивними. Тому у роботі розроблено критерії, за якими визначається прогресивність відповідних змін.

Досліджуються процеси змін рівня загальної безпеки системи в залежності від різних факторів, таких як точність вхідних даних задачі, точність реалізації алгоритму по відношенню до вимог, які описують особливості їх використання.

У розділі приводиться опис розробленої блок-схеми процесу управління функціонування та системи надання повноважень і досліджуються її можливості.

У розділі приводиться опис розробленої блок-схеми алгоритму загальної організації процесу функціонування системи *IS* в цілому.

Досліджуються відмінності між таким параметром системи, як її надійність та параметром, що характеризує безпеку.

Також проведено експериментальні дослідження, які показали, що позитивний результат від використання дворівневої моделі становить 19 відсотків.

Висновки

У дисертаційній роботі розв’язано нову науково-прикладну задачу щодо підвищення рівня захисту конфіденційних даних в інформаційних системах на основі використання моделі багаторівневої системи надання повноважень на отримання конфіденційних даних, що дозволяє уникнути дії негативних факторів щодо впливу на систему надання повноважень, які виникають на нижчих рівнях доступу до функціонально орієнтованих інформаційних систем.

При цьому отримано наступні наукові результати.

1. Проведено аналіз методів захисту систем доступу користувача до функціонально орієнтованих інформаційних систем, який показав неможливість отримання частини інформації з консолідованого блоку більш високого рівня конфіденційності та відсутністю дробових способів доступу, що суттєво перешкоджає проведенню аналізу великих масивів даних за малою вибіркою.

2. Удосконалено методи формального опису параметрів інформаційних моделей даних, які зберігаються в інформаційній системі, та дозволяють визначати їх величини, що дало змогу проводити їх оцінку відповідно до необхідного рівня конфіденційності, завдяки чому розширилися можливості використання їх в прикладних задачах.

3. Уперше розроблено метод визначення параметрів інформаційних запитів користувачів та обчислення їх величин, а також використовуючи характеристики конфіденційних даних з інформаційної системи стало можливим, незалежно від користувача, надавати задачі повноваження на використання конфіденційних даних, у цьому випадку задача виступає як окремий суб’єкт, що дозволяє уникнути можливого впливу користувача на отримання цих даних.

4. Розроблено метод визначення параметрів додаткових компонентів засобів доступу до інформаційної системи, який дозволив порівняти рівень конфіденційності даних з величинами параметрів інформаційних запитів задач, завдяки чому стало можливим модифікувати повноваження доступу задачі, що звернулася із запитом до інформаційних ресурсів.

5. Уперше розроблено компоненти, що складають дворівневу модель доступу до даних, у якій компоненти відповідних рівнів функціонують незалежно, але переходи з нижчого рівня на вищий реалізуються на основі перевірок, що проводяться на відповідному рівні, що дозволяє збільшити рівень безпеки системи доступу і, як наслідок, виключити можливість виникнення негативного впливу на предметну область задачі, що розв’язується.

6. Розроблено моделі, практична реалізація яких забезпечила проведення поглибленого аналізу запропонованих методів, який підтвердив адекватність отриманих результатів, що також підтверджено даними за результати впровадження.

7. Розроблено алгоритми надання повноважень та загальної організації роботи дворівневої системи захисту доступу до даних, що забезпечує елімінацію суб’єктивних факторів користувача, які могли б впливати на можливість доступу до конфіденційних даних, а також проведені експериментальні дослідження, які показали, що позитивний результат від використання дворівневої моделі становить 19 відсотків.

ЛІТЕРАТУРА

1. Петров А. А. Компьютерная безопасность. криптографические методы защиты / А. А. Петров. — М. : ДМК, 2000. — 445 с.

2. Зима В. М. Безопасность глобальных сетевых технологий / В. М. Зима, А. А. Молдовян, Н. А. Молдовян. — СПб. : БХВ-Петербург, 2000. — 320 с.

3. Озкарахан Э. Машины баз данных и управление базами данных / Э. Озкарахан. — М. : Мир, 1989. — 646 с.

4. Дрибас В. П. Реляционные модели баз данных / В. П. Дрибас. — Минск. : БГУ, 1982. — 297 с.

5. Суліма О. А. Аналіз основних систем надання повноважень користувачам / О. А. Суліма // Моделювання та інформаційні технології: Зб. наук. праць ІПМЕ НАН України. — 2017. — С. 90–97.

6. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии / О. Н. Василенко. — М. : МЦНМО, 2006. — 335 с.

7. Nyanchama M. Modeling mandatory access control in role-based security systems / M. Nyanchama, S. Osborn // InDBSec. — 1995. — P. 129–144.

8. Damgård I. Access control encryption: enforcing information flow with cryptography / I. Damgård, H. Haagh, C. Orlandi. — 2016.

9. Ionez A. K. Linear time algorithm for deciding security / A. K. Ionez, R. Lipton, I. Snyder // Symporium on Foundations of Computer Science. — 1976. — Vol. 17. — P. 492.

10. Bertino E. Access control for databases: concepts and systems / E. Bertino. — 2010. — 148 p.

11. Anisimov A. Variable-length prefix codes with multiple delimiters / A. Anisimov, I. Zavadskyi // IEEE Transactions on Information Theory. — 2017. — Vol. 63, № 5. — P. 2885–2895.

12. Rushby J. The bell and la padula security model / J. Rushby // Draft report, Computer Science Laboratory, SRI. — 1986. — P. 1–19.

13. Helkala K. Factors to affect improvement in cyber officer performance. / K. Helkala, B. Knox, Ø. Jøsok // Inf. & Comput. Security. — 2016. — Vol. 24, № 2. — P. 152–163.

14. Wangen G. An initial insight into information security risk assessment practices / G. Wangen, L. Tingliao, Z. A. Soomro // Information and Computer Security. — 2016. — Vol. 24, № 2. — P. 139–151.

15. Зайченко Ю. П. Нечеткие модели и методы в интеллектуальных системах / Ю. П. Зайченко. — К. : Слово, 2008. — 344 с.

16. Задірака В. К. Комп’ютерні технології криптографічного захисту інформації на спеціальних цифрових носіях / В. К. Задірака, А. М. Кудін, В. О. Людвиченко, О. С. Олексюк. — К. : Підручники і посібники, 2007. — 272 с.

17. Суліма О. А. Побудова моделі доступу на базі моделі діона / О. А. Суліма. — Тернопіль : 2017.

18. Dion L. C. A comlete protection model / L. C. Dion // Proceedings of the IEEE symposium on Security and Privacy. — 1981. — P. 49–55.

19. Cotrini C. Analyzing first-order role based access control / C. Cotrini, T. Weghorn, D. Basin, M. Clavel. — 2015.

20. Chang S. E. Exploring organizational culture for information security management / S. E. Chang, C. Lin // Industrial Management & Data Systems. — 2007. — Vol. 107, № 3. — P. 438–458.

21. Sandhu R. S. Role-based access control models / R. S. Sandhu, E. J. Coyne, U. I. Feinstein, C. I. Youmen // Computer. — 1996. — Vol. 29, № 2. — P. 38–47.

22. Ferreira A. How to securely break into rbac: the btg-rbac model / A. Ferreira, D. Chadwick, C. Farinha. — 2009.

23. Li Q. Towards secure dynamic collaborations with group-based rbac model / Q. Li, X. Zhang, M. Xu, J. Wu // Computers and Security. — 2009. — Vol. 28, № 5. — P. 260–275.

24. Yang K. Dac-macs: effective data access control for multi-authority cloud storage systems / K. Yang, X. Jia, K. Ren, B. Zhang // 2013 Proceedings IEEE INFOCOM. — 2013. — P. 2895–2903.

25. Coyne E. J. Abac and rbac: scalable, flexible, and auditable access management / E. J. Coyne, T. R. Weil // IT Professional. — 2013. — Vol. 15, № 3. — P. 14–16.

26. Ferrini R. Supporting rbac with xacml+owl / R. Ferrini, E. Bertino. — 2009.

27. Line M. B. Examining the suitability of industrial safety management approaches for information security incident management / M. B. Line, E. Albrechtsen // Information and Computer Security. — 2016. — Vol. 24, № 1. — P. 20–37.

28. Zhou Z.-Y. . b Hybrid mandatory integrity model composed of biba and clark-wilson policy / Z.-Y. . b Zhou, Y.-C. . He, H.-L. . Liang // Ruan Jian Xue Bao/Journal of Software. — 2010. — Vol. 21, № 1. — P. 98–106.

29. Al-Kahtani M. A. Rule-based rbac with negative authorization / M. A. Al-Kahtani, R. Sandhu. — 2004.

30. Kim S. A feature-based approach for modeling role-based access control systems / S. Kim, D.-K. Kim, L. Lu // Journal of Systems and Software. — 2011. — Vol. 84, № 12. — P. 2035–2052.

31. Li D. Rbac-based access control for saas systems / D. Li, C. Liu, Q. Wei. — 2010.

32. Сулима О. А. Основные тенденции развития киберпреступности на рубеже 2015 года / О. А. Сулима. — К. : ІПМЕ ім. Г.Є. Пухова НАНУ, 2015.

33. Давиденко А. Н. Анализ основных информационных компонент систем доступа / А. Н. Давиденко // Моделювання та інформаційні технології: Зб. наук. пр. — 2011. — Т. 59. — С. 11–20.

34. Marchenko O. Machine learning method for paraphrase identification / O. Marchenko, A. Anisimov, A. Nykonenko. — Springer, 2017.

35. Грофф Д. Р. Sql. полное руководство / Д. Р. Грофф, П. Н. Вайнберг, Э. Д. Оппелъ. — М. : Вильямс, 2015. — 959 с.

36. Ульман Д. Основы систем баз данных / Д. Ульман. — М. : Финансы и статистика, 1983. — 336 с.

37. Половко А. М. Основы теории надёжности / А. М. Половко, С. В. Гуров. — СпБ : БХВ-Петербург, 2006. — 704 с.

38. Мохор В. Функціональне моделювання системи керування ризиком безпеки інформації / В. Мохор, В. Цуркан, Я. Дорогий, О. Крук // Захист інформації. — 2016. — Т. 18, № 1. — С. 74–80.

39. Корченко А.О. Метод оцінки рівня критичності для систем управління кризовими ситуаціями / А.О. Корченко, В.А. Козачок, А.І. Гізун // Захист інформації. — 2015. — Т. 17, №. 1. — С. 86–98.

40. Корченко А. Г. Аналітичні вирази верифікації лінгвістичних змінних для систем оцінювання ризиків інформаційної безпеки / А. Г. Корченко, С. В. Казмирчук, Ф. А. Приставка, Б. Б. Ахметов // Безпека інформації. — 2017. — Т. 23, № 1. — С. 50–55.

41. Корченко А. Г. Анализ и оценивание рисков информационной безопасности / А. Г. Корченко, А. Е. Архипов, С. В. Казмирчук. — К. : Лазурит-Полиграф, 2013. — 275 с.

42. Корченко А. Г. Концептуальная модель и принципы обеспечения эффективности нейросетевого распознавания кибератак / А. Г. Корченко, И. А. Терейковский, Л. А. Терейковская // Інформаційні технології в економіці та природокористуванні. — 2017. — Т. 1, № 1.

43. Булинская Е. В. Теория риска и перестрахование / Е. В. Булинская. — М. : МГУ, 2001. — 119 с.

44. Бенинг В. Е. Введение в математическую теорию риска / В. Е. Бенинг, В. Ю. Королев. — М. : МАКС Пресс, 2001. — 184 с.

45. Терейковський І. А. Нейронні мережі в засобах захисту комп’ютерної інформації / І. А. Терейковський. — К. : Поліграф Консалтинг, 2007. — 209 с.

46. Новиков А. Н. Модели и методы кибернетической защиты информационно-коммуникационных систем на основе логико-вероятностного подхода / А. Н. Новиков, А. Н. Родионов, А. А. Тимошенко. — К. : Политехника, 2015. — 276 с.

47. Столлингс В. Основы защиты сетей. приложения и стандарты / В. Столлингс. — М. : Издательский дом “Вильямс,” 2002. — 432 с.

48. Мухачев В. А. Методы практической криптографии / В. А. Мухачев, В. А. Хорошко. — К. : Полиграф-Консалтинг, 2005. — 215 с.

49. Терейковський І. А. Формування політики безпеки комп’ютерних систем / І. А. Терейковський // Захист інформації. — 2008. — Т. 10, № 1. — С. 12–22.

50. Харченко В. П. Мультирівнева модель даних для ідентифікації забезпеченості вимог відповідно нормативно-правовому забезпеченню кібербезпеки цивільної авіації / В. П. Харченко, О. Г. Корченко, С. О. Гнатюк // Захист інформації. — 2017. — Т. 19, № 1. — С. 95–104.

51. Логінова Н. І. Правовий захист інформації / Н. І. Логінова, Р. Р. Дробожур. — Одеса : Фенікс, 2015. — 264 с.

52. Lomas E. Information governance: information security and access within a uk context / E. Lomas // Records Management Journal. — 2010. — Vol. 20, № 2. — P. 182–198.

53. Аверченков В. И. Системы защиты информации в ведущих зарубежных странах / В. И. Аверченков, М. Ю. Рытов, Г. В. Кондрашин, М. В. Рудановский. — Брянск : БГТУ, 2007. — 223 с.

54. Суліма О. А. Аналіз методів оцінок рівня безпеки доступу до даних / О. А. Суліма // Моделювання та інформаційні технології: Зб. наук. праць ІПМЕ НАН України. — 2017. — С. 80–87.

55. Павлов І. М. Проектування комплексних систем захисту інформації / І. М. Павлов, В. О. Хорошко. — Вінниця : ВНТУ, 2011. — 245 с.

56. Архипов А. Е. Практические аспекты оценивания рисков реализации угроз в информационных системах / А. Е. Архипов, А. В. Скиба // Захист інформації. — 2014. — Т. 16, № 3. — С. 215–222.

57. Андрєєв В. І. Основи інформаційної безпеки / В. І. Андрєєв, В. О. Хорошко, В. С. Чередніченко, М. Є. Шелест. — К. : ДУІКТ, 2009. — 292 с.

58. Бояринова Ю. Є. Технології захисту комп’ютерних систем і мереж / Ю. Є. Бояринова, А. Г. Корченко, И. А. Терейковский // Інформаційні технології в економіці та природокористуванні. — 2017. — Т. 1, № 1.

59. Борботько Т. В. Защита информации в банковских технологиях / Т. В. Борботько. — Мн. : БГУИР, 2006. — 125 с.

60. Диллон Б. Инженерные методы обеспечения надежности систем / Б. Диллон, Ч. Сингх. — М. : Мир, 1984. — 318 с.

61. Барлоу Р. Статистическая теория надежности и испытания на безотказность / Р. Барлоу, Ф. Прошан. — М. : Наука, 1984.

62. Архипов О. Є. Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації / О. Є. Архипов, А. В. Скиба // Захист інформації. — 2013. — Т. 15, № 4. — С. 366–375.

63. Ершов Ю. Л. Математическая логика / Ю. Л. Ершов, Е. А. Палютин. — М. : Наука, 1987. — 336 с.

64. Карри Х. Б. Основания математической логики / Х. Б. Карри. — М. : Мир, 1969. — 568 с.

65. Рутковская Д. Нейронные сети, генетические алгоритмы и нечеткие системы / Д. Рутковская, М. Пилиньский, Л. Рутковский. — М. : Телеком, 2006. — 385 с.

66. Королев В. Ю. Математические основы теории риска / В. Ю. Королев, В. Е. Бенинг, С. Я. Шоргин. — М. : Физматлит, 2011. — 591 с.

67. Хальд А. Математическая статистика с техническими приложениями / А. Хальд. — М. : Госиноиздат, 1956. — 664 с.

68. Мацнев А. П. Математическая логика и теория алгоритмов / А. П. Мацнев. — М. : МГАПИ, 2004. — 89 с.

69. Shih D. Securing industry-wide epc global network with ws-security / D. Shih, C. Sun, B. Lin // Industrial Management & Data Systems. — 2005. — Vol. 105, № 7. — P. 972–996.

70. Phillips C. E. Security assurance for an rbac/mac security model / C. E. Phillips, S. A. Demurjian, T. C. Ting. — 2003.

71. Гришина Н. В. Организация комплексной системы защиты информации / Н. В. Гришина. — М. : Гелиос АРВ, 2007. — 256 с.

72. Мендельсон Э. Введение в математическую логику / Э. Мендельсон. — М. : Наука, 1971. — 320 с.

73. Мышкис А. Д. Элементы теории математических моделей / А. Д. Мышкис. — М. : КомКнига, 2007. — 192 с.

74. Давиденко А. М. Використання формальних засобів опису процесів надання повноважень / А. М. Давиденко, О. А. Суліма // Захист інформації. — 2016. — Т. 18. — С. 143–149.

75. Зайченко Ю. П. Основи проектування інтелектаульних систем / Ю. П. Зайченко. — К. : Видавничий Дім «Слово», 2004. — 352 с.

76. Лазарев И. А. Информация и безопасность. композиционная технология информационного моделирования сложных объектов принятия решений / И. А. Лазарев. — М. : Московский городской центр научно-технической информации, 1997. — 336 с.

77. Зегжда Д. П. Как построить защищённую информационную систему / Д. П. Зегжда, А. М. Ивашко. — СПб. : Мир и семья, 1997. — 312 с.

78. Коростіль О. Ю. Аналіз методів інтерпретації текстових моделей / О. Ю. Коростіль // Моделювання та інформаційні технології: Зб. наук. праць ІПМЕ НАН України. — 2012. — Т. 62. — С. 47–58.

79. Коростіль О. Ю. Розширення параметрів текстових описів інформаційних потоків / О. Ю. Коростіль // Моделювання та інформаційні технології: Зб. наук. праць ІПМЕ НАН України. — 2012. — Т. 65. — С. 24–31.

80. Коротков М. А. Основы формальных логических языков / М. А. Коротков, Е. О. Степанов. — СПб. : ГИТМО, 2003. — 85 с.

81. Шенфилд Д. Математическая логика / Д. Шенфилд. — М. : Наука, 1975. — 528 с.

82. Смит Р. Э. Аутентификация: от паролей до открытых ключей / Р. Э. Смит. — М. : Вильямс, 2002. — 432 с.

83. Сачков В. Н. Введение в комбинаторные методы дискретной математики / В. Н. Сачков. — М. : МЦНМО, 2004. — 424 с.

84. Суліма О. А. Визначення оцінок параметрів в системі надання повноважень / О. А. Суліма. — К. : 2017.

85. Рейуорд-Смит В. Д. Теория формальных языков: вводный курс / В. Д. Рейуорд-Смит. — М. : Радио и связь, 1988. — 131 с.

86. Набебин А. А. Логика и пролог в дискретной математике / А. А. Набебин. — М. : МЭИ, 1996. — 452 с.

87. Макконнелл Д. Анализ алгоритмов / Д. Макконнелл. — М. : Техносфера, 2009. — 449 с.

88. Гасфилд Д. Строки, деревья и последовательности в алгоритмах / Д. Гасфилд. — СПб. : БХВ-Петербург, 2003. — 654 с.

89. Лавров С. С. Программирование. математические основы, средства, теория / С. С. Лавров. — СПб. : БХВ-Петербург, 2002. — 320 с.

90. Bell D. Secure computer systems: mathematical foundations / D. Bell, L. LaPadula. — Bedford : 1973. — 33 p.

91. Тапскотт Д. Электронно-цифровое общество: плюсы и минусы эпохи сетевого интеллекта / Д. Тапскотт. — К. : INT-пресс, 1999. — 406 с.

92. Тарасов В. Б. От многоагентных систем к интеллектуальным организациям / В. Б. Тарасов. — М. : Эдиториал, 2002. — 352 с.

93. Трофимова Е. А. Математические методы анализа / Е. А. Трофимова, С. В. Плотников, Д. В. Гилев. — Екатеринбург : Изд-во Урал. ун-та, 2015. — 272 с.

94. Соломатин Н. М. Информационные семантические системы / Н. М. Соломатин. — М. : Высшая школа, 1989. — 127 с.

95. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання / В. П. Горбулін, О. Г. Додонов, Д. В. Ланде. — К. : Інтертехнологія, 2009. — 164 с.

96. Цыпкин Я. З. Информационная теория идентификации / Я. З. Цыпкин. — М. : Наука, 1995. — 336 с.

97. Мельников В. П. Информационная безопасность и защита информации / В. П. Мельников. — М. : Издательский центр «Академия», 2008. — 336 с.

98. Гайкович В. Ю. Безопасность электронных банковских систем / В. Ю. Гайкович. — М. : Единая Европа, 1994. — 364 с.

99. Балакирский В. Б. Безопасность электронных платежей / В. Б. Балакирский // Конфидент. — 1996. — Т. 5. — С. 47–53.

100. Сабат В. І. Математичні моделі спеціалізованих семантичних аналізаторів / В. І. Сабат // Моделювання та інформаційні технології: Зб. наук. праць ІПМЕ НАН України. — 2003. — Т. 21. — С. 26–32.

101. Хорошко В. А. Методы и средства защиты информации / В. А. Хорошко, А. А. Чекатков. — К. : Юниор, 2003. — 504 с.

102. Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков. — К. : Видавнича група BHV, 2009. — 608 с.

103. Валькман Ю. Р. Модельно-параметрическое пространство: теория и применение / Ю. Р. Валькман, В. И. Гриценко, А. Ю. Рыхальский. — К. : Наукова думка, 2012. — 192 с.

104. Аляев Ю. А. Дискретная математика и математическая логика / Ю. А. Аляев, С. Ф. Тюрин. — М. : Финансы и статистика, 2006. — 368 с.

105. Суліма О. А. Модель багаторівневої системи доступу / О. А. Суліма // Безпека інформації. — 2017. — Т. 23. — С. 123–130.

106. Ахо А. Структуры данных и алгоритмы / А. Ахо, Д. Хопкрофт, Д. Ульман. — М. : Вильямс, 2003. — 382 с.

107. Богомолов А. М. Алгебраические основы теории дискретных систем / А. М. Богомолов, В. Н. Салий. — М. : Наука, 1997. — 368 с.

108. Левитин А. В. Алгоритмы: введение в разработку и анализ / А. В. Левитин. — М. : Вильямс, 2006. — 576 с.

109. Пентус А. Е. Теория формальных языков / А. Е. Пентус, М. Р. Пентус. — М. : МГУ, 2004. — 80 с.

110. Богданов А. М. Моделирование безопасной обработки информации в компьютерных системах / А. М. Богданов, А. В. Корнейко, Г. С. Корхмазов. — К. : Наук. думка, 2000. — 160 с.

111. Суліма О. А. Розробка алгоритму надання повноважень задачам на використання даних / О. А. Суліма // Моделювання та інформаційні технології: Зб. наук. праць ІПМЕ НАН України. — 2016. — Т. 77. — С. 110–116.

112. Суліма О. А. Аналіз впливу параметрів даних на процесі надання повноважень / О. А. Суліма // Моделювання та інформаційні технології: Зб. наук. праць ІПМЕ НАН України. — 2016. — Т. 76. — С. 110–118.

113. Суліма О. А. Аналіз процесів надання повноважень в інформаційно-телекомунікаційних системах / О. А. Суліма. — Харків : Технологічний центр, 2016.

114. Суліма О. А. Особливості використання засобів визначення повноважень в державних інформаційних системах / О. А. Суліма. — К. : ІПМЕ ім. Г.Є. Пухова НАНУ, 2016.

115. Редько В. Г. Эволюция, нейронные сети, интеллект : модели и концепции эволюционной кибернетики / В. Г. Редько. — М. : Ленанд, 2015. — 220 с.

116. Гладков Л. А. Генетические алгоритмы / Л. А. Гладков, В. В. Курейчик, В. М. Курейчик. — М. : ФИЗМАТЛИТ, 2006. — 320 с.

117. Акимов О. Е. Дискретная математика: логика, группы, графы, фракталы / О. Е. Акимов. — М. : АКИМОВА, 2005. — 656 с.

118. Алексеев В. Е. Графы. модели вычислений. структуры данных / В. Е. Алексеев. — Нижний Новгород : ННГУ, 2005. — 308 с.

119. Стахов А. П. Введение в алгоритмическую теорию измерения / А. П. Стахов. — М. : Сов. радио, 1977. — 117 с.

120. Уотшем Т. Д. Количественные методы в финансах / Т. Д. Уотшем, К. Паррамоу. — М. : Юнити, 1999. — 527 с.

121. Самохвалов Ю. Я. Экспертное оценивание. методический аспект / Ю. Я. Самохвалов, Е. М. Науменко. — К. : ДУІКТ, 2007. — 264 с.

122. Хованов Н. В. Анализ и синтез показателей при информационном дефиците / Н. В. Хованов. — СПб. : СПбГУ, 1994. — 196 с.

123. Кормен Т. Алгоритмы. построение и анализ / Т. Кормен, Ч. Лейзерсон, Р. Ривест, К. Штайн. — М. : Вильямс, 2013. — 1324 с.

124. Лейбин В. М. Глобалистика, информатизация, системные исследования / В. М. Лейбин. — М. : ЛКИ, 2007. — 295 с.

125. Морозов А. Д. Введение в теорию фракталов / А. Д. Морозов. — М. : Институт компьютерных исследований, 2002. — 162 с.

126. Сугак Е. В. Надежность технических систем / Е. В. Сугак, Н. В. Василенко. — Красноярск : НИИ, 2001. — 608 с.

127. Рябинин И. А. Надежность и безопасность структурно-сложных систем / И. А. Рябинин. — СПб. : Политехника, 2000. — 248 с.

128. Bertino E. Geo-rbac: a spatially aware rbac / E. Bertino, B. Catania // Proceedings of the tenth ACM symposium on Access control models and technologies. — 2005. — P. 29–37.

129. Глухов М. М. Введение в теоретико-числовые методы криптографии / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черёмушкин. — М. : Лань, 2011. — 400 с.

130. Доугерти К. Введение в эконометрику / К. Доугерти. — М. : ИНФРА-М, 2009. — 465 с.

131. Гуц А. К. Математическая логика и теория алгоритмов / А. К. Гуц. — Омск : Издательство Наследие, 2003. — 111 с.

132. Грибунин В. Г. Комплексная система защиты информации на предприятии / В. Г. Грибунин. — М. : Издательский центр «Академия», 2009. — 416 с.

Додаток А Лістінги (коди) програмних модулів

```
##########################################################################
#Реалізація дворівневої моделі доступу, для задачі проводження об’єкта без
#розголошення інформації більш високого рівня доступу.
#Розробник Суліма О.А.
#Мова реалізації Python 2.7
#Назва продукту Security Visualizer
#Версія v1.0 03.08.2017
#Copyright © Sulima, 2017
##########################################################################

# -*- coding: cp1251 -*-
# Python 2.7

import sys
import os
import subprocess
from PyQt5.QtCore import QCoreApplication, Qt
from PyQt5.QtGui import QIcon
from PyQt5.QtWidgets import QApplication, QWidget, QMainWindow, QPushButton,
QAction
from PyQt5.QtWidgets import QComboBox, QLabel
class window(QMainWindow):
    def __init__(self):
        super(window, self).__init__()
        self.setGeometry(200, 200, 150, 215)
        self.setWindowTitle('Меню')
        # self.setWindowIcon(QIcon('pic.png'))
```

```
    self.createUI()
    self.initVariables()
def createUI(self):
    aboutAction = QAction('&Про програму', self)
    aboutAction.setShortcut('F1')
    aboutAction.setStatusTip('Відкрити readme')
    aboutAction.triggered.connect(self.openReadme)
    self.statusBar()
    mainMenu = self.menuBar()
    infoMenu = mainMenu.addMenu('&Інфо')
    infoMenu.addAction(aboutAction)
        accessLevelLabel = QLabel('Рівень доступу', self)
    accessLevelLabel.move(25, 20)
    accessLevelComboBox = QComboBox(self)
    accessLevelComboBox.addItem('перший')
    accessLevelComboBox.addItem('другий')
    accessLevelComboBox.addItem('третій')
    accessLevelComboBox.addItem('четвертий')
    accessLevelComboBox.move(25, 45)
    accessLevelComboBox.activated[str].connect(self.setAccessLevel)
    accessColorLabel = QLabel('Колір', self)
    accessColorLabel.move(25, 85)
    accessColorComboBox = QComboBox(self)
    accessColorComboBox.addItem('червоний')
    accessColorComboBox.addItem('зелений')
```

```
        accessColorComboBox.addItem('синій')
        accessColorComboBox.addItem('жовтий')
        accessColorComboBox.move(25, 110)
        accessColorComboBox.activated[str].connect(self.setAccessColor)
        showMapButton = QPushButton('Показати карту', self)
        showMapButton.clicked.connect(self.showMap)
        showMapButton.move(25, 160)
        self.show()
    def initVariables(self):
        self.accessLevel = 'перший'
        self.accessColor = 'червоний'
    def setAccessLevel(self, text):
        self.accessLevel = text
    def setAccessColor(self, text):
        self.accessColor = text
    def showMap(self):
        subprocess.call(["visualizer.exe", self.accessLevel, self.accessColor])
    def openReadme(self):
        os.startfile('readme.txt')
if __name__ == "__main__":  # had to add this otherwise app crashed
    def run():
        app = QApplication(sys.argv)
        Gui = window()
        sys.exit(app.exec_())
run()
```

```
#########################################################################
#pathfinder.exe програма, яка знаходить на карті між двома заданими точками
#наближено найкоротший маршрут, який обминає кожну з чотирьох точок, які
#випадково згенеровано у просторі між початковою і кінцевою точками
#########################################################################
# -*- coding: cp1251 -*-
# Python 2.7
import sys
import geoplotlib
import pandas as pd
import numpy as np
import Queue

# --- load everything --- #
# settings
approachRadius = 0.03 # minimal distance a path has to keep from all green points
tileWidth = 0.02 # approximate size of tiles used for pathfinding
if len(sys.argv) >= 3:
    approachRadius = float(sys.argv[1])
    tileWidth = float(sys.argv[2])
experimentsAmount = 1
if len(sys.argv) == 4:
    experimentsAmount = int(sys.argv[3])
startPoint = pd.read_csv('data/start.csv')
```

```
endPoint = pd.read_csv('data/end.csv')

# center and spread for green points generation (lat, lon)

greensCenter = (startPoint.iat[0,1]+endPoint.iat[0,1])/2.0,
(startPoint.iat[0,2]+endPoint.iat[0,2])/2.0

gridSize = np.abs(startPoint.iat[0,1]-endPoint.iat[0,1]), np.abs(startPoint.iat[0,2]-
endPoint.iat[0,2])

greensSpread = gridSize[0]/2.0 - approachRadius, gridSize[1]/2.0- approachRadius

greens = pd.DataFrame(np.zeros(8).reshape(4,2), columns=['lat', 'lon'])

dumbRoute = pd.DataFrame(np.zeros(8).reshape(2,4), columns=['src_lat', 'src_lon',
'dest_lat', 'dest_lon'])

def experiment(): # returns dumb path length, smart path length and smart route dataframe


    # --- generate greens --- #

    greens['lat'] = np.random.uniform(greensCenter[0]-greensSpread[0],
greensCenter[0]+greensSpread[0], 4)

    greens['lon'] = np.random.uniform(greensCenter[1]-greensSpread[1],
greensCenter[1]+greensSpread[1], 4)

    # --- generate dumb route --- #

    dumbRoute.iat[0,0] = startPoint['lat']

    dumbRoute.iat[0,1] = startPoint['lon']

    dumbRoute.iat[0,2] = endPoint['lat']

    dumbRoute.iat[0,3] = startPoint['lon']

    dumbRoute.iat[1,0] = endPoint['lat']

    dumbRoute.iat[1,1] = startPoint['lon']

    dumbRoute.iat[1,2] = endPoint['lat']

    dumbRoute.iat[1,3] = endPoint['lon']

    # --- generate smart route --- #
```

```
    gridShape = int(gridSize[0]/(tileWidth*0.75)), int(gridSize[1]/tileWidth) # 75% factor for height to make the grid look more squared
    gridPivot = startPoint.iat[0,1], startPoint.iat[0,2]
    tileSize = gridSize[0] / (gridShape[0]-1), gridSize[1] / (gridShape[1]-1)
    tileStep = tileSize
    if (startPoint.iat[0,1] > endPoint.iat[0,1]):
        tileStep = tileStep[0] * -1,  tileStep[1]
    if (startPoint.iat[0,2] > endPoint.iat[0,2]):
        tileStep =  tileStep[0], tileStep[1] * -1
    passableTiles = pd.DataFrame(np.ones(gridShape)*-1) # -1 - passable, -2 - impassable
    def getMapCoordinates(tile, gridPivot, tileStep): #returns real map coordinates of a tile
        return (gridPivot[0] + tile[0]*tileStep[0], gridPivot[1] + tile[1]*tileStep[1])
    # calculate impassable tiles
    for y in range(gridShape[0]):
        for x in range(gridShape[1]):
            for g in range(4):
                gy = greens.iat[g,0]
                gx = greens.iat[g,1]
                dy = gridPivot[0] + y*tileStep[0] - gy
                dx = gridPivot[1] + x*tileStep[1] - gx
                if (np.sqrt(dx*dx + dy*dy) < approachRadius):
                    passableTiles.iat[y,x] = -2 # impassable
    def getNeighbors(tile, gridShape): # returns adjacent tiles on the grid
        neighbors = []
        neighbors.append((tile[0]+1,tile[1]+1)) # prioritize diagonal over orthogonal
        neighbors.append((tile[0]-1,tile[1]+1))
```

```
    neighbors.append((tile[0]-1,tile[1]-1))
    neighbors.append((tile[0]+1,tile[1]-1))
    neighbors.append((tile[0]+1,tile[1]))
    neighbors.append((tile[0],tile[1]+1))
    neighbors.append((tile[0]-1,tile[1]))
    neighbors.append((tile[0],tile[1]-1))
    goodNeighbors = []
    for t in neighbors:# filter neighbors that are out of the borders of the grid
        if (t[0] < 0 or t[1] < 0 or t[0] >= gridShape[0] or t[1] >= gridShape[1]):
            pass
        else:


            goodNeighbors.append(t)
    return goodNeighbors
# calculate distance to each tile
tileQueue = Queue.Queue()
tileQueue.put((0,0))
passableTiles.iat[0,0] = 0.0
while not tileQueue.empty():
    currTile = tileQueue.get()
    neighbors = getNeighbors(currTile, gridShape)
    for n in neighbors:
        if passableTiles.iat[n] == -2:
            continue # ignore impassable tiles
        distance = 1.0
```

```
            if (currTile[0]-n[0] + currTile[1]-n[1])%2 == 0:
                distance = 1.415 # distance is sqrt(2) for diagonal paths
            if (passableTiles.iat[n] == -1 or
                passableTiles.iat[n] > passableTiles.iat[currTile] + distance):
                passableTiles.iat[n] = passableTiles.iat[currTile] + distance
                tileQueue.put(n)


    # recreate path
    path = Queue.LifoQueue() # a stack, basically
    pathSize = 1 # amount of points in a path
    currTile = (gridShape[0]-1,gridShape[1]-1)
    smartPathLength = passableTiles.iat[currTile]
    path.put(getMapCoordinates(currTile, gridPivot, tileStep))
    while currTile != (0,0):
        neighbors = getNeighbors(currTile, gridShape)
        minDistance = smartPathLength
        for n in neighbors: # find closest neighbor
            if passableTiles.iat[n] < minDistance and passableTiles.iat[n] != -2:# closer and
passable
                minDistance = passableTiles.iat[n]
        for n in neighbors: # proceed to closest neighbor
            if passableTiles.iat[n] == minDistance:
                currTile = n
                path.put(getMapCoordinates(currTile, gridPivot, tileStep))
                pathSize += 1
                break
```

```
    # build route
    smartRoute = pd.DataFrame(np.zeros((pathSize-1)*4).reshape(pathSize-1,4),
columns=['src_lat', 'src_lon', 'dest_lat', 'dest_lon'])
    currPoint = path.get()
    for i in range(pathSize-1):
        nextPoint = path.get()
        smartRoute.iat[i,0] = currPoint[0]
        smartRoute.iat[i,1] = currPoint[1]
        smartRoute.iat[i,2] = nextPoint[0]
        smartRoute.iat[i,3] = nextPoint[1]
        currPoint = nextPoint
    dumbPathLength = gridShape[0] + gridShape[1] - 2.0
    return (smartPathLength, dumbPathLength, smartRoute)
# --- record distance --- #


experimentsData =
pd.DataFrame(np.zeros(experimentsAmount).reshape(experimentsAmount,1),
columns=['smart'])
for i in range(experimentsAmount):
    res = experiment()
    if (i == 0):
        dumbRouteLength = res[1]
    experimentsData.iat[i,0] = res[0]/dumbRouteLength
    #experimentsData.iat[i,1] = res[1]
    if (i == experimentsAmount-1):
        smartRoute = res[2]
with open('result.csv', 'w') as f:
```

```
        experimentsData.to_csv(f, line_terminator=',', index=False, header=False)
#experimentsData.to_scv('result.csv')


# --- plot everything --- #
label_color = [0,0,0,255]
geoplotlib.dot(startPoint, color=[255,0,0,255], point_size=5)
#geoplotlib.labels(startPoint, 'name', label_color, font_size=12, anchor_x='center')
geoplotlib.dot(endPoint, color=[0,0,255,255], point_size=5)
#geoplotlib.labels(endPoint, 'name', label_color, font_size=12, anchor_x='center')
geoplotlib.dot(greens, color=[0,255,0,255], point_size=3)
geoplotlib.graph(dumbRoute, src_lat='src_lat', src_lon='src_lon',
                 dest_lat='dest_lat', dest_lon='dest_lon',
                 color = 'hot_r', alpha=64, linewidth=2)
geoplotlib.graph(smartRoute, src_lat='src_lat', src_lon='src_lon',
                 dest_lat='dest_lat', dest_lon='dest_lon',
                 color = 'Greens', alpha=100, linewidth=3)
geoplotlib.show()
#pathfindermodel.exe програмне меню, яке дозволяє вибрати параметри запуску
#для pathfinder.exe
# -*- coding: cp1251 -*-
# Python 2.7


import sys
import os
import subprocess
from PyQt5.QtCore import QCoreApplication, Qt
```

```
from PyQt5.QtGui import QIcon
from PyQt5.QtWidgets import QApplication, QWidget, QMainWindow, QPushButton,
QAction
from PyQt5.QtWidgets import QComboBox, QLabel, QSlider
class window(QMainWindow):
    def __init__(self):
        super(window, self).__init__()
        self.setGeometry(200, 200, 150, 215)
        self.setWindowTitle('Меню')
        # self.setWindowIcon(QIcon('pic.png'))
        self.createUI()
        self.initVariables()
    def createUI(self):
        aboutAction = QAction('&Про програму', self)
        aboutAction.setShortcut('F1')
        aboutAction.setStatusTip('Відкрити readme')
        aboutAction.triggered.connect(self.openReadme)
        self.statusBar()
        mainMenu = self.menuBar()
        infoMenu = mainMenu.addMenu('&Інфо')
        infoMenu.addAction(aboutAction)

       approachRadiusLabel = QLabel('Радіус наближення', self)
        approachRadiusLabel.move(25, 20)
        approachRadiusSlider = QSlider(Qt.Horizontal, self)
        approachRadiusSlider.setFocusPolicy(Qt.NoFocus)
```

```
        approachRadiusSlider.setGeometry(25, 45, 100, 20)
        approachRadiusSlider.setMinimum(1)
        approachRadiusSlider.setMaximum(80)
        approachRadiusSlider.setValue(30)
        approachRadiusSlider.valueChanged[int].connect(self.changeApproachRadius)
        self.approachRadiusValueLabel = QLabel('0.030', self)
        self.approachRadiusValueLabel.move(25, 58)
        #accessLevelComboBox = QComboBox(self)
        #accessLevelComboBox.addItem('перший')
        #accessLevelComboBox.addItem('другий')
        #accessLevelComboBox.addItem('третій')
        #accessLevelComboBox.addItem('четвертий')
        #accessLevelComboBox.move(25, 45)
        #accessLevelComboBox.activated[str].connect(self.setAccessLevel)
        pathfinderResolutionLabel = QLabel('Точність', self)
        pathfinderResolutionLabel.move(25, 85)
        pathfinderResolutionSlider = QSlider(Qt.Horizontal, self)
        pathfinderResolutionSlider.setFocusPolicy(Qt.NoFocus)
        pathfinderResolutionSlider.setGeometry(25, 110, 100, 20)
        pathfinderResolutionSlider.setMinimum(5)
        pathfinderResolutionSlider.setMaximum(80)
        pathfinderResolutionSlider.setValue(10)
pathfinderResolutionSlider.valueChanged[int].connect(self.changePathfinderResolution)
        self.pathfinderResolutionValueLabel = QLabel('0.010', self)
        self.pathfinderResolutionValueLabel.move(25, 123)
```

```
        #accessColorComboBox = QComboBox(self)
        #accessColorComboBox.addItem('червоний')
        #accessColorComboBox.addItem('зелений')
        #accessColorComboBox.addItem('синій')
        #accessColorComboBox.addItem('жовтий')
        #accessColorComboBox.move(25, 110)
        #accessColorComboBox.activated[str].connect(self.setAccessColor)
        showMapButton = QPushButton('Показати карту', self)
        showMapButton.clicked.connect(self.showMap)
        showMapButton.move(25, 160)
        self.show()
    def initVariables(self):
        self.approachRadius = 0.03
        self.pathfinderResolution = 0.01
    def changeApproachRadius(self, value):
        self.approachRadius = 0.001 * value
        self.approachRadiusValueLabel.setText("{:.3f}".format(self.approachRadius))
    def changePathfinderResolution(self, value):
        self.pathfinderResolution = 0.001 * value
self.pathfinderResolutionValueLabel.setText("{:.3f}".format(self.pathfinderResolution))
    def showMap(self):

        subprocess.call(["pathfinder.exe", str(self.approachRadius),
str(self.pathfinderResolution)])
    def openReadme(self):
        os.startfile('readme.txt')
```

```
if __name__ == "__main__":  # had to add this otherwise app crashed
    def run():
        app = QApplication(sys.argv)
        Gui = window()
        sys.exit(app.exec_())
run()
##########################################################################
#graph.exe програма побудови графіків
##########################################################################
import numpy as np
import matplotlib.pyplot as plt
data = np.genfromtxt('result.csv', delimiter=',')
data = data[:-1].copy()
low = 0.0
high = 1.0
step = 0.02
frequency = np.zeros(int((high-low)/step))
for sample in data:
    index = int((sample-low)/step)
    frequency[index] += 1
plt.plot(np.arange(len(frequency))*step+low, frequency)
plt.show()
##########################################################################
#visualizer.exe програма, яка відображає карту з точками, до яких має доступ
#користувач
##########################################################################
```

```
# -*- coding: cp1251 -*-
# Python 2.7
import sys
import geoplotlib
import pandas as pd
#from geoplotlib.utils import read_csv
if len(sys.argv) == 3:
    levels = {'перший': 1, 'другий': 2, 'третій': 3, 'четвертий': 4}
    accessLevel = levels.get(str(sys.argv[1]), 1)
    accessColor = str(sys.argv[2])
else:

    accessLevel = 1
    accessColor = 'червоний'
allRed = pd.read_csv('data/red.csv')
showedRed = allRed[allRed['accesslevel'] >= accessLevel].reset_index()
allGreen = pd.read_csv('data/green.csv')
showedGreen = allGreen[allGreen["accesslevel"] >= accessLevel].reset_index()
allBlue = pd.read_csv('data/blue.csv')
showedBlue = allBlue[allBlue["accesslevel"] >= accessLevel].reset_index()
allYellow = pd.read_csv('data/yellow.csv')
showedYellow = allYellow[allYellow["accesslevel"] >= accessLevel].reset_index()
label_color = [0,0,0,255]
if accessColor == 'червоний':
    geoplotlib.dot(showedRed, color=[255,0,0,255])
```

```
    geoplotlib.labels(showedRed, 'name', label_color, font_size=12, anchor_x='center')
if accessColor == 'зелений':
    geoplotlib.dot(showedGreen, color=[0,255,0,255])
    geoplotlib.labels(showedGreen, 'name', label_color, font_size=12, anchor_x='center')
if accessColor == 'синій':
    geoplotlib.dot(showedBlue, color=[0,0,255,255])
    geoplotlib.labels(showedBlue, 'name', label_color, font_size=12, anchor_x='center')
if accessColor == 'жовтий':
    geoplotlib.dot(showedYellow, color=[200,200,0,255])
    geoplotlib.labels(showedYellow, 'name', label_color, font_size=12, anchor_x='center')
geoplotlib.show()
```

Додаток Б Документи, що підтверджують впровадження результатів дисертаційної роботи

ЗАТВЕРДЖУЮ

Учений секретар
доктор фіз.-мат. наук
_____ С. В. ЄРШОВ
«__»_____ 2017 р.

АКТ

впровадження результатів дисертаційної роботи Суліми Олександра Андрійовича «Методи та моделі захисту інформаційних ресурсів на основі багаторівневої моделі організованого доступу» на здобуття наукового ступеню кандидата технічних наук у діяльності Інститут кібернетики імені В.М.Глушкова Національної академії наук України

Даний акт складено про те, що результати дисертаційної робіти Суліми Олександра Андрійовича «Методи та моделі захисту інформаційних ресурсів на основі багаторівневої моделі організованого доступу» впроваджено та використовано у діяльності Інститут кібернетики імені В.М.Глушкова Національної академії наук України при проведенні первинної державної експертизи комплексної системи захисту інформації Національного ресурсного центру.

У процесі написання дисертації автором було розроблено та досліджено компоненти, що складають дворівневу модель захисту даних, в якій компоненти відповідних рівнів функціонують незалежно, але переходи з нижчого рівня на вищий реалізуються на основі перевірок, що проводяться на нижчому рівні, які призначені для збільшення міри захисту таємних даних і, як наслідок (ввести додаткові вищі рівні таємності даних та виключити можливість доступу до таких даних процесів нижчого рівня захисту).

Таким чином, результати, отримані Сулімою О.А. при написанні дисертації, дозволили використовувати системи оцінювання ризиків безпеки інформаційних ресурсів в умовах великих осягів консолідованої інформації та підвищити ефективність і рівень автоматизації процесів управління ризиками при побудові комплексних систем захисту інформації та систем менеджменту інформаційної безпеки.

Завідувач лабораторії
канд.техн. наук А. Л. Головинський

ЗАТВЕРДЖУЮ

Проректор з навчальної та виховної роботи Національного авіаційного університету

_____ І. Іванова

«02» 08 2017 р.

АКТ

впровадження у навчальний процес Національного авіаційного університету результатів дисертаційної роботи Суліма Олександр Андрійович «МЕТОДИ ТА МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ НА ОСНОВІ БАГАТОРІВНЕВОЇ МОДЕЛІ ОРГАНІЗОВАНОГО ДОСТУПУ» на здобуття наукового ступеня кандидата технічних наук.

Комісія у складі: голова –завідувача кафедри безпеки інформаційних технологій (БІТ) Корченко О.Г., члени комісії – професор кафедри БІТ Іванченко Є.В. та доцент кафедри БІТ Жмурко Т.О., склали цей акт про те, що результати дисертаційної роботи Суліма Олександр Андрійович «Методи та моделі захисту інформаційних ресурсів на основі багаторівневої моделі організованого доступу» впроваджені у навчальний процес і використовуються на кафедрі БІТ при викладанні наступних дисциплін: «Теорія ризику», «Менеджмент інформаційної безпеки», «Комплексні системи захисту інформації» та «Управління інформаційною безпекою». Дані дисципліни викладаються при підготовці бакалаврів спеціальності 125 «Кібербезпека» (освітні програми «Адміністративний менеджмент у сфері захисту інформації» та «Системи технічного захисту, автоматизація її обробки»).

№ з/п	Назва роботи, що впроваджується	Форма впровадження	Ефективність від впровадження
	1	2	3
1.	Дворівневу модель захисту даних, в якій компоненти відповідних рівнів функціонують не залежно, але переходи з нижчого рівня на вищий реалізуються на основі перевірок, що проводяться на нижчому рівні (аналітична модель характеристик захисту даних)	Лекція	Ознайомлення студентів з аналітична модель характеристик захисту даних, яка використовує додаткові вищі рівні таємності даних для забезпечення можливості доступу до таких даних процесів нижчого рівня захисту.
2.	Методи формального опису параметрів даних, що зберігаються в системі доступу	Лекція	Ознайомлення студентів з методами формального опису параметрів даних, що зберігаються в системі доступу до ресурсів інформаційних систем.

Голова комісії,
завідувача кафедри безпеки інформаційних технологій О. Корченко

Члени комісії:

професор кафедри безпеки інформаційних технологій Є.Іванченко

доцент кафедри безпеки інформаційних технологій Т.Жмурко