НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ ІМ. Г. Є. ПУХОВА

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Кваліфікаційна наукова
праця на правах рукопису

ДАВИДЕНКО АНАТОЛІЙ МИКОЛАЙОВИЧ

УДК 004.056.52:004.056.53:004.75 (043.3)

ДИСЕРТАЦІЯ

МЕТОДИ ТА МОДЕЛІ АДАПТИВНОГО ЗАХИСТУ ТА РОЗМЕЖУВАННЯ ДОСТУПУ ДО РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Спеціальність: 05.13.21 – «Системи захисту інформації»
Галузь знань: 12 – «Інформаційні технології»

Подається на здобуття наукового ступеня доктора технічних наук

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

А. М. Давиденко

Науковий консультант: **Корченко Олександр Григорович**, доктор технічних наук, професор, лауреат Державної премії України в галузі науки і техніки, завідувач кафедри безпеки інформаційних технологій Національного авіаційного університету

Київ – 2021

АНОТАЦІЯ

Давиденко А.М. Методи та моделі адаптивного захисту та розмежування доступу до розподілених інформаційних ресурсів. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 «Системи захисту інформації». – Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України, Національний авіаційний університет, Київ, 2021.

Розвиток інформаційних технологій, крім прогресу, породжує також нові протиріччя. Відомі та апробовані механізмі захисту в нових умовах можуть вже не задовольняти сучасним потребам. Тому актуальним є аналіз сучасного стану інформаційних систем з метою удосконалення механізмів їх функціонування.

Метою роботи є забезпечення процесу декомпозиції розмежування доступу до розподілених інформаційних ресурсів, шляхом адаптації системи захисту до поточного стану безпеки кібердовкілля, що обумовлюється вирішенням науково-технічної проблеми породженою об’єктивним протиріччям між існуючою потребою в багатопотоковому доступі до розподілених інформаційних ресурсів грід-систем, з одного боку, та централізованою однопотоковою архітектурою існуючих засобів захисту, з іншого.

Для досягнення поставленої мети, необхідно розв’язати наступні задачі: провести аналіз відомих методів розмежування доступу до ресурсів інформаційних систем та дослідити відповідні математичні моделі з метою виявлення можливостей їх використання для захисту розподілених інформаційних ресурсів; удосконалити моделі нейронних мереж для забезпечення керування розмежуванням доступу; розробити метод самоорганізації засобів розмежування доступу; розробити та дослідити основні інформаційні компоненти розширення функціоналу засобів розмежування доступу до інформаційних ресурсів; розробити метод адаптації системи розмежування доступу для розподілених інформаційних ресурсів відповідно до поточного стану безпеки кібердовкілля; розробити методи аналізу стану безпеки систем розмежування доступу; розробити

модель та окремі компоненти засобів системи розмежування доступу; провести експериментальні дослідження запропонованих методів, моделей та систем.

Для вирішення поставлених задач спочатку були проаналізовані сучасні методи та моделі розмежування доступу до ресурсів інформаційних систем. Встановлено, що однопотокові механізми розмежування доступу не можуть забезпечити високі вимоги для високопродуктивної обробки інформаційних ресурсів з обмеженим доступом, в той же час спостерігається постійне зростання продуктивності обчислювальних систем, тому запропоновано наділити підсистему захисту властивостями адаптації по відношенню до критеріїв, які визначаються параметрами стану безпеки системи та параметрами, що характеризують процеси обробки інформації у спеціалізованих розподілених інформаційних системах.

В рамках дисертаційного дослідження удосконалено структурну модель нейрона. Модель нейрона була розширена введенням додаткового блоку пам’яті та блоку аналізу. Зазначені блоки комутуються до блоку підсумовування вхідних параметрів та формують зворотний зв’язок з функціональними змінними нейрона. Зазначена модель дозволяє в межах окремого нейрона запам’ятовувати часовий тренд його вагових параметрів на визначеному часовому інтервалі, завдяки чому з’являється новий функціонал організації контролю даних в системах розмежування доступу.

В роботі розглянуто завдання розпізнання нових атак і завдання збільшення ефективності розпізнання атак, яке використовує сигнатури атак, на основі використання такої властивості нейронних мереж, як властивість її самоорганізації, яка є вищим за рівнем методів зміни можливостей мережі в порівнянні з методами навчання. На наступному етапі дисертаційних досліджень отримав подальший розвиток метод самоорганізації засобів розмежування доступу, в якому за рахунок застосування правила Хебба та відповідної модифікації адаптаційної залежності, для випадку формування вхідних сигналів, які не містять постійної складової, сформовано співвідношення для побудови рекурентного алгоритму на базі односпрямованої нейронної мережі.

Однією з важливих особливостей використання різних типів нейронних мереж є необхідність у використанні досить розвинутої інформаційної системи, що відображала б всі необхідні, для функціонування нейронних систем, дані. Крім того, в межах відповідної інформаційної системи повинні існувати засоби, які забезпечували б попередню обробку відповідних даних, перш ніж останні можна було б подавати у функціональні блоки, які реалізовані на основі використання нейронних мереж.

Цілком очевидно, що інформаційна система повинна ґрунтуватися на описах предметних областей, які описують інтерпретацію даних, що використовуються у всіх фрагментах системи. Тому, в роботі, розглянуто основні компоненти системи, які необхідні для вирішення задач інформаційного забезпечення системи безпеки. До таких компонентів віднесемо наступні: словники, що містять опис базових елементів предметних областей; система синтаксичних правил формування описів інтерпретації базових елементів; система семантичних параметрів, які характеризують особливості інтерпретації базових елементів і інших компонентів; система семантичних правил, які регламентують способи побудови опису інтерпретації елементів, які використовуються при функціонуванні системи; система правил перетворення описів компонентів системи.

Найбільш низьким рівнем абстракції буде володіти мова, що будується на основі базових компонентів, що описують найбільш широко розповсюджену предметну область. При використанні такого способу визначення зміни рівня абстракції мови, може мати місце ситуація, коли дві різні предметні області, які використовують різні базові елементи по відношенню один до одного, мають максимальні рівні абстракції. Для виключення можливості виникнення такої суперечливості сформульовано відповідні умови. В цілому за рахунок сюр’єкції множин ідентифікаторів предметних областей користувачів та об’єктів доступу формуються бієкції та набір семантичних правил, що узагальнює процес вирішення завдання побудови взаємозворотних перетворень.

В роботі проведено дослідження взаємозв'язків між семантичними

параметрами. Введено наступні семантичні параметри, які будуть характеризувати семантику інформаційних засобів системи, які допускають текстове відображення природною мовою: семантична значимість елемента; семантична ефективність елемента; суперечливість фрагмента; погодженість фрагментів у пропозиції; рівень конфліктності пропозицій.

В роботі визначено що процесом адаптації є процес, що регламентується наступними правилами: процес адаптації може робити зміни оцінки значень аналізованих параметрів; процес адаптації не здійснює зміни логіки алгоритмів аналізу контрольованих параметрів; процес адаптації може змінювати кількість аналізованих параметрів, якщо це не приводить до змін логіки аналізу окремих параметрів.

В останньому розділи наведені приклади реалізації запропонованих в роботі методів та моделей, а саме: дві системи біометричної автентифікації користувачів інформаційних систем, за клавіатурним та за рукописним почерком; апаратно-програмний комплекс підтримки прийняття рішень при проведенні державних експертиз комплексних систем захисту інформації; грід-сервіс віддаленого синтезу конфігурацій для реконфігуровних засобів захисту інформації Security Tasks Reconfigurable Accelerators Grid-Service на базі гріду та хмарної інфраструктури Українського національного гріду.

До наукової новизни та практичної цінності, які були отримані в результаті дисертаційних досліджень, можна віднести наступне.

Удосконалено структурну модель нейрона, в якій за рахунок інтегрування додаткового блоку пам’яті та блоку аналізу, які комутуються до блоку підсумовування вхідних параметрів та формують зворотний зв’язок з функціональними змінними нейрона, реалізується новий функціонал організації контролю даних в системах розмежування доступу.

Отримав подальший розвиток метод самоорганізації засобів розмежування доступу, в якому за рахунок застосування правила Хебба та відповідної модифікації адаптаційної залежності, для випадку формування вхідних сигналів, які не містять постійної складової, сформовано співвідношення для побудови

рекурентного алгоритму на базі односпрямованої нейронної мережі.

Вперше розроблено структурну модель засобів інформаційного забезпечення системи розмежування доступу, в якій за рахунок сюр'єкції множин ідентифікаторів предметних областей користувачів та об'єктів доступу формуються бієкції та набір семантичних правил, що узагальнює процес вирішення завдання побудови взаємозворотних перетворень.

Вперше запропоновано метод адаптації системи розмежування доступу, в якому за рахунок генерування зміни оцінки значень параметрів та регулювання їх кількості при збереженні логіки аналізу, система розмежування доступу набуває нового функціоналу автоматичного інкременту або декременту кількості механізмів захисту при відповідній варіабельності стану безпеки ресурсів інформаційних систем.

Удосконалено метод аналізу системи розмежування доступу, який за рахунок консолідації оцінок рівня захищеності індивідуальних елементів об'єкта доступу, множини загроз, множини зв'язків із зовнішнім оточенням, функціонального завантаження об'єкта доступу та параметру навантаження обчислювальних ресурсів дозволив отримати комплексну оцінку стану безпеки.

Вперше розроблено структурно-функціональну декомпозиційну модель системи розмежування доступу, яка за рахунок блоків аналізу результатів реалізованого доступу, аналізу ситуації відмови в доступі, критеріїв адаптації засобів захисту відповідно до поточного стану безпеки кібердовкілля та керування засобами захисту системи доступу, дозволяє реалізувати запропонований метод адаптації системи розмежування доступу, шляхом розробки та рекомбінації окремих компонентів системи розмежування доступу до розподілених інформаційних ресурсів.

Розроблені в роботі моделі та методи адаптації засобів захисту, використовувались при реалізації систем контролю доступу, окремих механізмів захисту та побудові моделей загроз та порушника, а також програм та методик випробувань при проведенні державних експертиз комплексних систем захисту за дорученням ДССЗЗІ СБУ України.

Розроблено програми та методики випробувань при проведенні державних експертиз комплексних систем захисту інформації: Центру реєстрації віртуальних організацій української національної грід-інфраструктури Київського національного університету імені Тараса Шевченка, Українського академічного грід-вузла Інституту теоретичної фізики ім. М.М. Боголюбова Національної академії наук України, автоматизованої інформаційної системи Президії Національної академії наук України, автоматизованої системи класу «2» Ресурсного центру Інституту кібернетики Національної академії наук України, локальної обчислювальної мережі Управління справами Національної академії наук України, автоматизованої системи класу «2» для підготовки даних Департаменту військово-технічної політики, розвитку озброєння та військової техніки Міністерства оборони України, автоматизованої системи для обробки відкритої інформації Центрального науково-дослідного інституту озброєння та військової техніки Збройних Сил України.

Модифіковано алгоритми використання ресурсів мережевої інфраструктури на базі проміжного програмного забезпечення Nordugrid ARC, яке є базовим для Українського національного гріду.

Розроблено грід-сервіс віддаленого синтезу конфігурацій для реконфігуровних засобів захисту інформації Security Tasks Reconfigurable Accelerators Grid-Service на базі гріду та хмарної інфраструктури Українського національного гріду.

Розроблено апаратно-програмний комплекс підтримки прийняття рішень при проведенні державних експертиз комплексних систем захисту інформації.

Розроблено апаратно-програмний комплекс моніторингу та керування технологічним процесом зневоднення бішофіту.

Розроблені в дисертаційній роботі методи побудови засобів захисту на основі використання математичних моделей використовувались в науково-дослідних роботах, що проводились в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України за темами «Кріт», «МодА», «МодБ», «МодД», «Управление», «Модель» та виконувались у відповідності з замовленням Президії

академії наук України, а також у роботах за цільовими комплексними програмами.

Результати дисертації впроваджено у діяльність Інституту кібернетики імені В.М. Глушкова Національної академії наук України, ТОВ «Софтлайн ІТ», НДЦ «Нафтогазбурмаш», Департаменту військово-технічної політики, розвитку озброєння та військової техніки Міністерства оборони України, Центральному науково-дослідному інституту озброєння та військової техніки Збройних Сил України, а також використовувалась в навчальному процесі Київського національного університету імені Тараса Шевченка, Національного авіаційного університету для підготовки фахівців з кібербезпеки.

Експериментальні дослідження програмних застосунків безпеки систем розмежування доступу та інших розробок, а також їх впровадження і успішне практичне використання, підтвердили достовірність теоретичних положень і висновків дисертаційної роботи.

Ключові слова: контроль доступу, захист інформації, розподілені інформаційні системи, ідентифікація, автентифікація, авторизація.

ABSTRACT

Davydenko A. Methods and models of adaptive protection and differentiation of access to distributed information resources. – Qualifying scientific work as a manuscript.

Thesis for a Doctor of Technical Sciences degree in the specialty 05.13.21 - «Information Security Systems». – Pukhov Institute for Modelling in Energy Engineering NAS of Ukraine, National Aviation University. Kyiv, 2021.

The development of information technology, in addition to progress, also generates new contradiction. Well-known and tested protection mechanisms in the new conditions may no longer meet modern needs. Therefore, the analysis of the current state of information systems in order to improve the mechanisms of their functioning is relevant.

The purpose of the work is to ensure the process of decomposing the separation of access to distributed information resources by adapting the protection system to the current state of cyber-environment security, which is caused by the solution of the scientific and technical problem generated by the objective contradiction between the existing need for multi-threaded access to distributed information resources of Grid systems, on the one hand, and the centralized one-threaded architecture of existing protection means, on the other hand.

To achieve this goal, it is necessary to solve the following tasks: to analyze the known methods of differentiation of access to information systems resources and to investigate the relevant mathematical models in order to identify the possibilities of their use to protect distributed information resources; improve neural network models to ensure access separation control; to develop a method of self-organization of means of differentiation of access; to develop and investigate the main information components of expanding the functionality of means of differentiation of access to information resources; develop a method for adapting the access separation system for distributed information resources in accordance with the current state of cyber-environment

security; develop methods for analyzing the security status of access separation systems; develop a model and separate components of the access delimitation system.

Programs and methods of testing during state examinations of complex information protection systems have been developed: the Center for Registration of Virtual Organizations of the Ukrainian National Grid Infrastructure of Taras Shevchenko National University of Kyiv, the Ukrainian Academic Grid Node of the Institute for Theoretical Physics. M.M. Bogolyubov of the National Academy of Sciences of Ukraine, automated information system of the Presidium of the National Academy of Sciences of Ukraine, automated class "2" system of the Resource Center of the Institute of Cybernetics of the National Academy of Sciences of Ukraine, local computer network case management of the National Academy of Sciences of Ukraine, automated system class "2" for the preparation of data of the Department of Military-Technical Policy, development of weapons and military equipment of the Ministry of Defense of Ukraine, automated system for processing open information central research

The algorithms for using network infrastructure resources based on Nordugrid ARC intermediate software, which is the base for the Ukrainian National Grid, have been modified.

The grid service of remote synthesis of configurations for reconfigurable information protection means Security Tasks Reconfigurable Accelerators Grid-Service based on grid and cloud infrastructure of the Ukrainian National Grid was developed.

The hardware and software complex of decision support during state examinations of complex information protection systems has been developed.

The hardware and software complex for monitoring and management of the technological process of bischofite dehydration has been developed.

The methods of construction of protective equipment developed in the dissertation work on the basis of the use of mathematical models were used in research works carried out at the Institute of Problems of Modeling in the Energy Sector. G.E. Pukhova NAS of Ukraine on the topics " Mod ", " ModA ", "ModB", " ModD ", "Management", "Model" and was carried out in accordance with the order of the Presidium of the Academy of Sciences of Ukraine, as well as in the works on targeted complex

programs.

The results of the dissertation were introduced in the activities of the Institute of Cybernetics named after V.M. Glushkov of the National Academy of Sciences of Ukraine, Softline IT LLC, Naftogazburmash SSC, the Department of Military And Technical Policy, the Development of Weapons and Military Equipment of the Ministry of Defense of Ukraine, the Central Research Institute of Armament and Military Equipment of the Armed Forces of Ukraine, and was used in the educational process of Taras Shevchenko National University of Kyiv, the National Aviation University for the training of specialists in cybersecurity.

Experimental studies of software security applications of access delimitation systems and other developments, as well as their implementation and successful practical use, confirmed the reliability of theoretical provisions and conclusions of the dissertation work.

One of the important features of using the system of different types of neural networks is the need to use a sufficiently developed information system that would reflect all the data necessary for the functioning of neural systems. In addition, within the relevant information system, there must be tools that would ensure the preliminary processing of relevant data before the latter can be submitted to functional blocks that are implemented on the basis of the use of neural networks.

It is obvious that the information system should be based on descriptions of subject areas that describe the interpretation of data used in all fragments of the system. Therefore, the work considers the main components of the system, which are necessary to solve the problems of information support of the security system. These components include the following: dictionaries containing a description of the basic elements of subject areas; system of syntax rules for forming descriptions of interpretation of basic elements; a system of semantic parameters that characterize the peculiarities of interpretation of basic elements and other components; a system of semantic rules that regulate ways to build a description of the interpretation of elements used in the functioning of the system; system rules for converting descriptions of system components.

The lowest level of abstraction will be the language built on the basis of the basic components describing the most widespread subject area. When using this method of determining the change in the level of speech abstraction, there may be a situation when two different subject areas that use different basic elements in relation to each other have maximum levels of abstraction. To exclude the possibility of such a contradiction, appropriate conditions have been formulated. In general, due to the surreality of sets of identifiers of subject areas of users and access objects, bjections and a set of semantic rules are formed, which summarizes the process of solving the problem of constructing adversary transformations.

The research of the relationship between semantic parameters was carried out. The following semantic parameters have been introduced that will characterize the semantics of the information means of the system, which allow text display in natural language: semantic significance of the element ; semantic effectiveness of the element; fragment contradiction; approval of fragments in the proposal; level of conflict of proposals .

The work defines that the process of adaptation is a process regulated by the following rules: the adaptation process can make changes in the evaluation of the values of the analyzed parameters; the adaptation process does not change the logic of the algorithms for analyzing controlled parameters; the adaptation process can change the number of parameters analyzed, unless it changes the logic of the analysis of individual parameters.

The last section provides examples of the implementation of the methods and models proposed in the work, namely: two systems of biometric authentication of users of information systems, by keyboard and handwriting; hardware and software complex of decision support during state examinations of complex information protection systems; remote configuration synthesis service for reconfigurable information security tools Security Tasks Reconfigurable Accelerators Grid-Service based on grid and cloud infrastructure of the Ukrainian National Grid.

The scientific novelty and practical value that were obtained as a result of dissertation research include the following.

The structural model of the neuron has been improved, in which, by integrating an

additional memory block and an analysis unit that is switching to the input parameters summation unit and forming feedback with functional variables of the neuron, a new functionality of data control organization in access delimitation systems is implemented.

He received further development of the method of self-organization of means of differentiation of access, in which due to the application of the Hebb rule and the corresponding modification of adaptation dependence, in the case of the formation of input signals that do not contain a permanent component, a ratio was formed to build a recurrent algorithm based on a unidirectional neural network.

For the first time, a structural model of means of information support of the access delimitation system was developed, in which, due to the surreality of sets of identifiers of substantive areas of users and access objects, biomes and a set of semantic rules are formed, which summarizes the process of solving the problem of constructing adversary transformations.

For the first time, a method of adaptation of the access delimitation system was proposed, in which by generating a change in the evaluation of parameters and adjusting their number while maintaining the logic of analysis, the access delimitation system acquires a new functionality of automatic increment or decrement of the number of protection mechanisms with the appropriate variability of the security state of information systems resources.

The method of analysis of the access delimitation system was improved, which, due to the consolidation of assessments of the level of security of individual elements of the access object, the set of threats, the set of connections with the external environment, the functional loading of the access object and the load parameter of computational resources, allowed to obtain a comprehensive assessment of the security state.

For the first time, a structural and functional decomposition model of the access delimitation system was developed, which, due to blocks of analysis of the results of realized access, analysis of the situation of access denial, criteria for adaptation of protection means in accordance with the current state of cyber-environment security and management of access system protection means, allows to implement the proposed

method of adaptation of the access delimitation system, through the development and recombination of individual components of the system of delimitation of access to distributed information resources.

The models and methods of adaptation of protective equipment developed in the work were used in the implementation of access control systems, individual protection mechanisms and the construction of threats and violator models, as well as programs and methods of testing during state examinations of complex protection systems on behalf of the SSSZZI of the Security Service of Ukraine.

Programs and methods of testing during state examinations of complex information protection systems have been developed: the Center for Registration of Virtual Organizations of the Ukrainian National Grid Infrastructure of Taras Shevchenko National University of Kyiv, the Ukrainian Academic Grid Node of the Institute for Theoretical Physics. M.M. Bogolyubov of the National Academy of Sciences of Ukraine, automated information system of the Presidium of the National Academy of Sciences of Ukraine, automated class "2" system of the Resource Center of the Institute of Cybernetics of the National Academy of Sciences of Ukraine, local computer network case management of the National Academy of Sciences of Ukraine, automated system class "2" for the preparation of data of the Department of Military-Technical Policy, development of weapons and military equipment of the Ministry of Defense of Ukraine, automated system for processing open information central research

The algorithms for using network infrastructure resources based on Nordugrid ARC intermediate software, which is the base for the Ukrainian National Grid, have been modified.

The grid service of remote synthesis of configurations for reconfigurable information protection means Security Tasks Reconfigurable Accelerators Grid-Service based on grid and cloud infrastructure of the Ukrainian National Grid was developed.

The hardware and software complex of decision support during state examinations of complex information protection systems has been developed.

The hardware and software complex for monitoring and management of the technological process of bischofite dehydration has been developed.

The methods of construction of protective equipment developed in the dissertation work on the basis of the use of mathematical models were used in research works carried out at the Institute of Problems of Modeling in the Energy Sector. G.E. Pukhova NAS of Ukraine on the topics "Mole", "Fashion", "ModB", "Fashion", "Management", "Model" and was carried out in accordance with the order of the Presidium of the Academy of Sciences of Ukraine, as well as in the works on targeted complex programs.

The results of the dissertation were introduced in the activities of the Institute of Cybernetics named after V.M. Glushkov of the National Academy of Sciences of Ukraine, Softline IT LLC, Naftogazburmash SSC, the Department of Military And Technical Policy, the Development of Weapons and Military Equipment of the Ministry of Defense of Ukraine, the Central Research Institute of Armament and Military Equipment of the Armed Forces of Ukraine, and was used in the educational process of Taras Shevchenko National University of Kyiv, the National Aviation University for the training of specialists in cybersecurity.

Experimental studies of software security applications of access delimitation systems and other developments, as well as their implementation and successful practical use, confirmed the reliability of theoretical provisions and conclusions of the dissertation work.

Keywords: access control, information security, distributed information systems, identification, authentication, authorization.

Список основних публікацій здобувача

1. В. Бабак, В. Харченко, А. Давиденко та ін., *Безпека авіації: Колективна монографія*. За ред. В. Бабака, К.: Техніка, 2004, С. 584.

2. A. N. Davydenko, S. Yu. Kravets, V. V. Mokhor, «Properties of systems of basis functions constructed using simple digit functions», *Izvestiya Vysshikh Uchebnykh Zavedenij. Radioelektronika*, vol. 38, №11-12, pp. 58-62, 1995.

3. A. N. Davydenko, S. Yu. Kravets, V. V. Mokhor, «On specificity of application of various logical bases for constructing mathematical models of nonlinear objects using complex bitwise functions», *Engineering Simulation*, vol. 13, № 2, pp. 317-326, 1995.

4. O. Vysotska, A. Davydenko, «Keystroke Pattern Authentication of Computer Systems Users as One of the Steps of Multifactor Authentication», *Advances in Computer Science for Engineering and Education II. Advances in Intelligent Systems and Computing*, vol. 938, pp. 356-368, 2019.

5. A. Davydenko, O. Vysotska, T. Shmelova, «Methods of Primary Processing Handwriting Samples at User Authentication Using a Probabilistic Neural Network*», 1st International Conference on Cyber Hygiene and Conflict Management in Global Information Networks (CyberConf 2019)*, Kyiv, Ukraine, 2019., pp. 723-735.

6. A. Davydenko, «Formalization level of abstraction of state information resourses access systems», *Scientific letters of academic society of Michel Baludansky*, vol.4, no. 1, pp. 35-38, 2016.

7. O. Vysotska, A. Davydenko, «Authentication of information systems users, based on the analysis of their handwriting», *Scientific and Practical Cyber Security Journal (SPCSJ)*, vol.2, no.4, pp. 51-63, 2018.

8. А. Давиденко, О. Суліма, «Використання формальних засобів опису процесів надання повноважень», *Захист інформації*, Том 18, №2, С.143-149, 2016.

9. В. Евдокимов, А. Давиденко, С. Гильгурт, «Централизованный синтез реконфигурируемых аппаратных средств информационной безопасности на

высокопроизводительных платформах», *Захист інформації*, Том. 20, № 4, С.247-258, 2018.

10. О. Корченко, А. Давиденко, О. Висоцька, «Метод автентифікації користувачів інформаційних систем за їх рукописним почерком з багатокроковою корекцією первинних даних», *Захист інформації*, Том 21, №1, С. 40-51, 2019.

11. О. Корченко, А. Давиденко, М. Шабан, «Декомпозиційна модель представлення смислових констант та змінних для реалізації експертиз у сфері ТЗІ», *Захист інформації*, Том 21, № 2, С. 88-96, 2019.

12. О. Корченко, А. Давиденко, М. Шабан, «Модель параметрів для ідентифікації функціонального профілю захисту в комп'ютерних системах», *Безпека інформації*, Том 25, № 2, С.122-126, 2019.

13. О. Корченко, А. Давиденко, М. Шабан, І. Іванченко, «Метод ідентифікації функціонального профілю захисту», *Захист інформації*, Том 21, № 4, С.252-258, 2019.

14. А. Корченко, А. Давиденко, М. Шабан, С. Казмірчук, «Структурна модель СППР при проведенні державних експертиз КСЗІ», *Безпека інформації*, Том 26, № 1, С.14-27, 2020.

15. А. Н. Давиденко, «Математическое моделирование систем и средств защиты критической информации», *Збірник наукових праць інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України*, Вип. 4, С. 109-113, 1998.

16. А. Н. Давиденко, «Анализ критериев безопасной обработки информации в КС», *Моделювання та інформаційні технології. Зб. наук. праць*, Вип. 3, С. 155-160, 1999.

17. А. Н. Давиденко, «Организационные и технологические проблемы криптографической защиты», *Моделювання та інформаційні технології. Зб. наук. праць*, Вип. 4, С. 10-14, 1999.

18. А. Н. Давиденко, «Вероятностная оценка надежности реализации функций защиты информации», *Моделювання та інформаційні технології. Зб. наук. праць*, Вип. 14, С. 64-70, 2002.

19. А. Н. Давиденко, «Исследование возможностей стандартов безопасности информации», *Збірник наукових праць інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України*, Вип. 15, С. 118-122, 2002.

20. А. Н. Давиденко, «Базовые требования к методологии построения угроз для информации с ограниченным доступом в автоматизированных системах», *Збірник наукових праць інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України*, Вип. 17, С. 150-154, 2002.

21. А. Н. Давиденко, Е. А. Высоцкая, «Современное состояние методологии анализа рисков при обеспечении информационной безопасности компьютерной системы», *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: Зб. наук. праць*, Вип. 4, С. 43-49, 2002.

22. А. Н. Давиденко, «Проблемы анализа и моделирования национальных и международных критериев оценки безопасности информации», *Збірник наукових праць інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України*, Вип. 18, С. 171-175, 2002.

23. А. Н. Давиденко, «Анализ средств защиты баз данных», *Моделювання та інформаційні технології. Зб. наук. праць*, Вип. 20, С. 137-141, 2003.

24. А. Н. Давиденко, «Использование ИТ – технологий при автоматизации процесса управления документами», *Збірник наукових праць інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України*, Вип. 20, С. 142-147, 2003.

25. А. М. Давиденко, «Проблеми обробки документів за допомогою офісних засобів в аспекті безпеки інформаційного обміну», *Збірник наукових праць інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України*, Вип. 21, С. 94-99, 2003.

26. Е. Высоцкая, А. Давиденко, «Исследование эффективности применения вероятностных нейронных сетей для решения задачи аутентификации пользователя компьютерных систем», *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Наук.-техн. зб.*, Вип. 9, С. 103-110, 2004.

27. А. Н. Давиденко, «Исследование параметров нейронных сетей характеризирующих их функциональные возможности», *Збірник наукових праць інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України*, Вип. 37, С. 118-126, 2006.

28. А. Н. Давиденко, «Исследование методов обучения нейронных сетей для решения задач противодействия атакам на систему управления доступом», *Збірник наукових праць інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України*, Вип. 40, С. 114-122, 2007.

29. А. Н. Давиденко, «Расширение теоретических возможностей математических моделей нейронных сетей обуславливаемых их использованием для решения задач защиты систем доступа», *Збірник наукових праць інституту проблем моделюваня в енергетиці ім. Г.Є. Пухова НАН України*, Вип. 45, С. 112- 115, 2008.

30. А. Н. Давиденко, Б. В. Дурняк, В. И. Сабат, «Обучение нейронных моделей средств защиты систем доступа», *Моделювання та інформаційні технології. Зб. наук. праць*, Вип. 47, С. 118-126, 2008.

31. А. Н. Давиденко, Б. В. Дурняк, «Методы реализации процесса обучения нейронных сетей для решения задач формирования профилей пользователей», *Збірник наукових праць інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України*, Вип. 48, С. 132-140, 2008.

32. А. Н. Давиденко, Б. В. Дурняк, «Исследование методов самоорганизации нейронных систем для решения задач распознавания атак», *Збірник наукових праць інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України*, Вип. 49, С. 106-116, 2008.

33. Е. А. Высоцкая, А. Н. Давиденко, «Анализ технологии предварительной обработки данных при аутентификации пользователей компьютерных систем по клавиатурному и рукописному почеркам», *Моделювання та інформаційні технології. Зб. наук. праць*, Вип. 55, С. 34-41, 2010.

34. А. Н. Давиденко, «Анализ основных информационных компонент систем доступа», *Моделювання та інформаційні технології. Зб. наук. праць*, Вип. 59, С.11-20, 2011.

35. А. Н. Давиденко, М. Р. Шабан, «Разработка методики проведения экспертизы комплексных систем защиты информации», *Моделювання та інформаційні технології. Зб. наук. праць*, Вип. 73, С.114-221, 2014.

36. А. Н. Давиденко, «Исследование взаимосвязей между семантическими параметрами для области безопасности систем доступа», *Моделювання та інформаційні технології. Зб. наук. праць*, Вип. 78, С.21-30, 2017.

37. А. М. Давиденко, О. А. Суліма, О. А. Давиденко, «Використання дворівневої моделі доступу до даних для вирішення прикладної задачі з проведення об'єкту по території з обмеженим доступом», *Моделювання та інформаційні технології. Зб. наук. праць*, Вип. 80, С.95-100, 2017.

38. В. Ф. Евдокимов, А. Н. Давиденко, С. Я. Гильгурт, «Организация централизованной генерации файлов конфигураций для аппаратных ускорителей задач информационной безопасности», *Моделювання та інформаційні технології. Зб. наук. праць*, Вип. 81, С.3-11, 2017.

39. А. М. Давиденко, О. А. Суліма, «Структурні підходи до методів оцінки рівня безпеки інформаційних систем», *Моделювання та інформаційні технології. Зб. наук. праць*, Вип. 83, С.11-21, 2018.

40. А. М. Давиденко, О. А. Суліма, «Аналіз функціональних можливостей окремих компонент засобів захисту інформаційних систем», *Моделювання та інформаційні технології. Зб. наук. праць*, Вип. 84, С.103-111, 2018.

41. А.М. Давиденко, С.Я. Гільгурт, М.Р. Шабан, «Апаратно-програмний комплекс підтримки прийняття рішень при проведенні державних експертиз комплексних систем захисту інформації», *Патент UA 139730 U; G06F17/27*. Патент опубліковано 10.01.2020, бюл. № 1.

42. А. М. Давиденко, С. Я. Гільгурт, О. О. Політучій, «Апаратно-програмний комплекс моніторингу та керування технологічним процесом зневоднення бішофіту», *Патент UA 140326 U; G05B15/00, G05B19/00.* Патент опубліковано 10.02.2020, Бюл. № 3.

43. А. Н. Давиденко, В. В. Шорошев, О. С. Потенко, «Оценка профилей противодействия угрозам на основе динамического программирования с

использованием принципа оптимума Р.Беллмана», Моделювання: XXIX Науково-технічна конференція, Київ, 2010, С. 33.

44. А. Н. Давиденко, М. Р. Шабан, «Разработка тестов для анализа информационной безопасности национальной грид-инфраструктуры», *XXXIII науково-технічна конференція молодих вчених та спеціалістів*, Київ, 2014, с.11.

45. А. Н. Давиденко, «Анализ условий изменения количества параметров в адаптивных системах защиты информации», *Problems and perspectives in European education development: International scientific and practical conference*, Prague, Czech Republic, 2016, pp.103-104.

46. А. М. Давиденко, «Методи та моделі функціонування адаптивних засобів захисту доступу до інформаційних систем», Актуальні питання забезпечення кібербезпеки та захисту інформації: ІІІ Міжнародна науково-практична конференція, Київ, 2017, с.69-70.

47. A. Salnikov, A. Davydenko, «Web-service for FPGA synthesis using ARC-powered grid infrastructure», *Annual NorduGrid Conference 2017*, Tromsø, Norway, 2017.

48. O. Vysotska, A. Davydenko, «The usage of handwriting recognition systems of information systems users for their authentication», *La science et la technologie à l'ère de la société de l'information: conférence scientifique et pratique internationale*, Bordeaux, France, 2019, vol.9, pp.48-51.

49. О. Висоцька, А. Давиденко, В. Щербина, «Формалізація процедури аналізу рукописного почерку людини для організації розмежування доступу до інформаційних систем», *ITSec: Безпека інформаційних технологій: IX Міжнародна науково-технічна конф.*, Київ (Україна), Шарм-ель-Шейх (Египет), 2019, С.22-23.

50. А. Н. Давыденко, С. Я. Гильгурт, «Применение грид-сети для синтеза промышленных систем защиты информации на базе ПЛИС», *Цифровые технологии в промышленности: республиканской научно-практической конференции*, Актау, Казахстан, 2019. С.15-20.

51. А. М.Давиденко, О. О.Висоцька, «Визначення функції моніторингу стану санкціонованих користувачів комп’ютерних систем за допомогою аналізу їх клавіатурного почерку», *Комп'ютерні системи та мережні технології (CSNT-2019): XII Міжнародна науково-практична конф.*, Київ, 2019, С.41-42.

52. А. М.Давиденко, О. О.Висоцька, «Моніторинг функціонального стану представників критичних професій, за допомогою аналізу їх клавіатурного почерку», *Актуальні проблеми управління інформаційною безпекою держави: X Всеукраїнська науково-практична конференція*, Київ, 2019, С.201-203.

53. A. Davydenko, O. Sulima, O. Vysotska, S. Hilgurt, «A study case of the implementation of a multi-layered access system to manage the procedures for using confidential information without violating the security policy», *Захист інформації і безпека інформаційних систем: VII Міжнародна науково-технічна конференція*, Львів, 2019, С.27-28.

54. А. М. Давиденко, О. А. Суліма, О. О. Політучий, «Реалізація процесів адаптації при вирішенні завдань захисту систем доступу до інформаційних об’єктів енергетики», *Кібербезпека енергетики*: *науково-практична конференція*, Одеса, 2019, С.16-20.

55. М. Р. Шабан, М. П. Карпінський, О. Г. Корченко, А. М. Давиденко, «Розробка методу ідентифікації функціональних профілей захисту», *Актуальні питання забезпечення кібербезпеки та захисту інформації: VI Міжнародна науково-практична конференція*, Київ, 2020, С.113-116.

56. О. Корченко, А. Давиденко, М. Шабан, «Формування критеріїв для функціонального профілю захисту», *ITSec: Безпека інформаційних технологій: X Міжнародна науково-технічна конференція*, Київ (Україна), Шарм-ель-Шейх (Египет), 2020, С.35-36.

57. А. М. Давиденко, М. Р. Шабан, В. П. Щербина, «Структурна модель СППР для проведення експертиз КСЗІ», *Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS’2020): XII Всеукраїнська науково-практична конференція*, Коблево, 2020, С.19-20.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

OGSA	–	Open Grid Services Architecture
OGF	–	Open Grid Forum
GT	–	Globus Toolkit
УНГ	–	Український національний грід
РППЗ	–	розподілений програмний застосунок користувача
MPI	–	Message Passing Interface
ОС	–	операційна система
WMS	–	Workload Management System
MD	–	Data Management System
SE	–	Storage Element
CS	–	Catalog Services
DS	–	Data Scheduler
R-GMA	–	Relational Grid Monitoring Architecture
GSI	–	Grid Security Infrastructure
LB	–	Logging and Bookkeeping
CE	–	Computing Element
ВО	–	віртуальна організація
EGI	–	європейська грід ініціатива
DAC	–	Discretionary access control
MAC	–	Mandatory access control
ABAC	–	Attribute-Based Access Control
NBAC	–	autheNtication-Based Access Control
ZBAC	–	authoriZation-Based Access Control,
IBAC	–	Identity-Based Access Control
ACL	–	Access Control List
RBAC	–	Role-Based Access Control
XACML	–	EXtensible Access Control Markup Language
NLP	–	Natural Language Policy
DP	–	digital policies

MP	–	metapolicy
PEP	–	Policy Enforcement Point
PIP	–	Policy Information Point
PAP	–	Policy Administration Point
CBAC	–	Context-based access control
LBAC	–	Lattice-based access control
D	–	типи доступу, що використовуються в моделі
E	–	компонент безпеки
S	–	системний компонент
R+	–	Read, write, create, delete операції над об’єктами специфічної структури
R–	–	обмеження R/W
Z	–	обмеження накладаються на найпростіші операції r/w
X	–	операції read, write можуть бути видаленими
C	–	забезпечує однорідний контроль права на доступ над неоднорідною безліччю 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 впорядковані відповідно до рівнів безпеки
M	–	крім найпростіших операцій в моделі можуть з’явитися операції, спрямовані на специфічну обробку інформації
P	–	можливість підключення паралельного механізму розмежування доступу
K	–	наявність мультипотокового механізму захисту
H	–	наявність ієрархії рівнів доступу
КНОІ	–	канал несанкціонованого отримання інформації
NGNs	–	Next Generation Networks
AAO	–	Authentication, Authorization and Accounting

IR	–	інформаційні ресурси
SD	–	система керування доступом
ARD	–	аналіз результатів реалізованого доступу
AOD	–	аналіз ситуації у випадку, коли в доступі користувачеві відмовлено
FR	–	формування рішень для засобів захисту за поточним станом системи доступу
UZD	–	керування засобами захисту системи доступу до інформаційних ресурсів
SZD	–	система захисту доступу.
АКРП	—	метод автентифікації користувачів інформаційних систем за їх рукописним почерком
АМОД	—	метод розпізнавання, який заснований на аналізі математичного очікування та дисперсії
АМОДДЗ	—	метод розпізнавання, який заснований на аналізі математичного очікування та дисперсії, з виконанням додаткового зважування
АРКНПЗК	—	метод розпізнавання, який заснований на аналізі ритму клавіатурного набору з пропорційним завданням класів
АРКНПРЗК	—	метод розпізнавання, який заснований на аналізі ритму клавіатурного набору з пороговим завданням класів
АСХ	—	метод розпізнавання, який заснований на аналізі статистичних характеристик
АСХФПФ	—	метод розпізнавання, який заснований на аналізі статистичних характеристик для фіксованої парольної фрази
АФЩРІВЗ	–	метод розпізнавання, який заснований на аналізі функції щільності розподілу імовірностей випадкових змінних
БДНЗ	–	база даних навчальних зразків
БС	–	біометричні системи
АКРП	–	метод автентифікації користувачів інформаційних систем за їх рукописним почерком

АМОД – метод розпізнавання, який заснований на аналізі математичного очікування та дисперсії

АМОДДЗ – метод розпізнавання, який заснований на аналізі математичного очікування та дисперсії, з виконанням додаткового зважування

АРКНПЗК – метод розпізнавання, який заснований на аналізі ритму клавіатурного набору з пропорційним завданням класів

АРКНПРЗК – метод розпізнавання, який заснований на аналізі ритму клавіатурного набору з пороговим завданням класів

АСХ – метод розпізнавання, який заснований на аналізі статистичних характеристик

АСХФПФ – метод розпізнавання, який заснований на аналізі статистичних характеристик для фіксованої парольної фрази

АФЩРІВЗ – метод розпізнавання, який заснований на аналізі функції щільності розподілу імовірностей випадкових змінних

БДНЗ – база даних навчальних зразків

БС – біометричні системи

АКРП – метод автентифікації користувачів інформаційних систем за їх рукописним почерком

АМОД – метод розпізнавання, який заснований на аналізі математичного очікування та дисперсії

АМОДДЗ – метод розпізнавання, який заснований на аналізі математичного очікування та дисперсії, з виконанням додаткового зважування

АРКНПЗК – метод розпізнавання, який заснований на аналізі ритму клавіатурного набору з пропорційним завданням класів

АРКНПРЗК – метод розпізнавання, який заснований на аналізі ритму клавіатурного набору з пороговим завданням класів

АСХ – метод розпізнавання, який заснований на аналізі статистичних характеристик

ВСТУП

Актуальність теми. Однією з сучасних тенденцій розвитку інформаційних систем є розподілена обробка інформації. Розвиток апаратної бази породжує паралельні обчислювальні середовища, використання яких істотно прискорює і в ряді випадків здешевлює процес обробки інформації. Прикладом паралельного обчислювального середовища є спеціалізовані розподілені мережі типу грід або розподілені мережі загального призначення типу хмара. В обох випадках існують проблема захисту інформаційних ресурсів та проблеми попередження їх пошкоджень. Це обумовлено практичною необхідністю уникати втрат, до яких можуть приводити несанкціоноване використання інформаційних ресурсів людини та суспільства, а також несанкціоноване використання інформації, яка знаходиться в цих ресурсах. Остання обставина є особливо важливою у зв'язку з тим, що засоби обчислювальної техніки та комп'ютерні мережі широко використовуються для створення інформаційних ресурсів, а відповідна інформація знаходить застосування для вирішення цілої гами завдань прикладного характеру. Прикладом таких завдань можуть служити задачі управління банківськими системами, управління складними технологічними процесами в промисловості, задачі, що існують у військовій галузі та ціла низка інших задач.

Більшість інформаційних ресурсів реалізується на базі комп'ютерних мереж, що представляють собою системи колективного використання, в рамках яких забезпечується доступ до мереж великої кількості користувачів. Це визначає необхідність досліджувати та розв'язувати задачі розвитку методів функціонування систем захисту інформації для побудови теоретичної, методологічної, технічної, технологічної та організаційної основи створення відповідних засобів захисту доступу до розподілених інформаційних систем.

На сьогоднішній день, найбільш поширеними методами захисту доступу є методи, що ґрунтуються на автентифікації користувачів та шифрування даних. Нажаль практичний досвід тестування грід систем доводить неефективність наявних засобів доступу. Очевидно, що використання однопотокового

шифрування веде до колапсу процесу паралельного вирішення завдань, а попереднє розшифрування даних робить їх уразливими. Тому для подолання цієї суперечності необхідно дослідити та вирішити проблему, яка пов’язана з находженням балансу між продуктивністю системи та рівнем безпеки, який вона забезпечує. В цьому випадку системи доступу потребують, щоб система захисту була гнучкою, що дозволило би керувати рівнем захисту в системі доступу в процесі функціонування обчислювальної мережі. Важливою проблемою, що потребує вирішення при проектуванні засобів захисту для системи доступу, є реалізація таких засобів захисту, які могли б самостійно підлаштовуватись до тих чи інших змін, які відбуваються за потребами користувачів відповідної системи. В цьому випадку виникають задачі розпізнавання санкціонованих або легальних користувачів, задачі адаптації параметрів засобів захисту та системи захисту в цілому до зовнішніх змін, що відбуваються у користувачів. З іншого боку, приймаючи до уваги, що засоби захисту, в залежності від рівня захисту, який вони забезпечують, мають різну вартість та споживають різну кількість ресурсів обчислювальної мережі та приймаючи до уваги інші фактори, може виявитися, що та чи інша інформація з часом змінює необхідний рівень її захисту. В цьому випадку, доцільно таким чином проектувати засоби захисту системи доступу, щоб автоматично, незалежно від адміністратора мережі, міг би змінюватися рівень захисту, який ці засоби забезпечують. З викладеного випливає, що засоби захисту, яким притаманні наведені вище властивості, повинні будуватися на основі теоретичного апарату та таких інструментальних засобів, які б у максимально можливій мірі забезпечували б реалізацію необхідних алгоритмів розв’язання перерахованих задач. Одним з таких інструментальних засобів, які в найбільшій мірі могли б забезпечити можливість розв’язання згаданих задач, є нейронні мережі.

У дисертаційній роботі розв’язана та досліджена науково-технічна проблема, що полягає у вирішенні протиріччя між необхідністю високопродуктивної обробки інформаційних ресурсів з обмеженим доступом, паралельна обробка яких висуває високі вимоги до швидкості їх підготовки, але однопотокові механізми

розмежування доступу не можуть їх забезпечити, тому пропонується розробити методи та моделі, які здатні узгоджувати продуктивність методів обробки та захисту та адаптувати їх один до одного для високопродуктивного та безпечного існування в розподіленому інформаційному кібердовкіллі, що дозволяє отримати нові рішення науково-технічних задач формування системи розмежування доступу до інформаційних ресурсів людини, суспільства та держави на основі використання моделей захисту, що за допомогою оперативного налаштування процесу контролю розмежування доступу, в тому числі на основі нейронних мереж, дозволило наділити відповідну підсистему захисту властивостями адаптації по відношенню до критеріїв, які визначаються параметрами рівня безпеки системи та параметрами, що характеризують процеси обробки інформації у спеціалізованих розподілених інформаційних системах.

Дослідженню проблем, пов’язаних із процесом обробки та розмежування доступу до інформації у спеціалізованих розподілених інформаційних системах, що є об’єктом дисертаційного дослідження присвячується значна частина публікацій вітчизняних і зарубіжних вчених, таких як: Д. Зегжда, В. Герасименко, К. Касперскі, Whitfield Diffie, Martin Hellman, David Elliott Bell, Leonard J. LaPadula, Carl E. Landwehr, David D. Clark та інші. Однак, незважаючи на значну кількість підходів до вирішення даної проблеми, вона залишається актуальною не тільки для України, але і для всієї світової спільноти.

Зв'язок роботи з науковими програмами, планами, темами. Дослідження, що проводились, при виконанні дисертаційної роботи виконувались у відповідності з планом науково-дослідних робіт Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України в рамках наступних науково-дослідних тем: НДР «Кріт» «Розробка методів побудови та формального опису критеріїв оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу» № 0101U006700 (2001р.-2004р.). НДР «МодА» «Дослідження і розробка методів розпізнавання, які базуються на використанні спектральних перетворень, для інформаційного забезпечення безпеки енергетичних об’єктів» № 0105U001296 (2005р.-2008р.). НДР «Управление» «Розробка методів і

комп’ютерних засобів підтримки прийняття рішень в задачах ситуаційного і технологічного управління в енергетиці» № 0102U005589 (2002р.-2006р.). НДР «Модель» «Розвиток теорії, розробка нових методів і засобів математичного й комп'ютерного моделювання енергетичних і енергоємних об'єктів, систем і установок» № 0107U001945 (2007р.-2009р.). НДР «МодБ» «Исследование и разработка методов повышения безопасности и эффективности распределенных высокопроизводительных информационных технологий при решении задач энергетики» №0108U010588 (2009р.-2013р.). НДР «МодД» «Дослідження та розробка методів оцінювання захищеності інформації в розподілених високопродуктивних інформаційних системах при вирішенні задач енергетики» № 0114U002361 (2014р.-2018р.). НДР «МодЕ» «Дослідження ризиків інформаційної безпеки об’єктів критичної інфраструктури ГТС України та розробка методології поводження з ними» № 0118U002371 (2019р.-по теперішній час). НДР «ГІБРИД» «Розвиток теорії, розробка методів та засобів реалізації гібридних експертно-моделюючих комп’ютерних систем в задачах комплексного управління перетворенням енергії» № 0112U000050 (2012р.-2016р.). НДР «НОВІНТЕХ» «Розвиток теорії, розробка новітніх інформаційних технологій в задачах комплексного моделювання та управління процесами перетворення та використання енергії» №0117U004347 (2017р.-по теперішній час). НДР «ГРІДІПМЕМОН-11» «Створення грід-системи моніторингу, збору та аналізу даних в енергетичній галузі на базі грід-центру з питань енергетики» №0111U004339 (2011р.-2013р.), згідно Державної цільової науково-технічної програми впровадження і застосування грід-технологій на 2009-2013 роки. НДР «ГРІДІПМЕМОН-15» «Підтримка та розвиток грід-сайту Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАНУ, як ресурсного центра NGI_UA, та створення грід-сервіса централізованого синтезу конфігурацій для апаратних прискорювачів задач інформаційної безпеки в енергетичній галузі» №0115U002876 (2015р.), згідно Цільової комплексної програми наукових досліджень НАН України «Грід-інфраструктура і грід-технології для наукових і науково-прикладних застосувань». НДР «ГРІДІПМЕМОН-16» «Підтримка та

розвиток грід-сайту Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАНУ та створення системи централізованого програмування реконфігуровних прискорювачів задач інформаційної безпеки в енергетичній галузі» №0116U006907 (2016р.), згідно Цільової комплексної програми наукових досліджень НАН України «Грід-інфраструктура і грід-технології для наукових і науково-прикладних застосувань». НДР «ГРІДІПМЕМОН-18» «Підтримка грід-сайту Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАНУ та використання хмарної інфраструктури для централізованого програмування реконфігуровних засобів інформаційної безпеки в енергетичній галузі» №0118U001370 (2018р.), згідно Цільової комплексної програми наукових досліджень НАН України «Грід-інфраструктура і грід-технології для наукових і науково-прикладних застосувань». НДР «ГРІДІПМЕМОН-19» «Підтримка грід-сайту ІПМЕ ім. Г.Є. Пухова НАН України та модернізація веб-сервісу централізованого програмування реконфігуровних засобів інформаційної безпеки на базі гріду та хмарної інфраструктури» №0119U001812 (2019р.), згідно Програми інформатизації НАН України на 2019р. НДР «ГРІДІПМЕМОН-20» «Підтримка грід-сайту ІПМЕ ім. Г.Є. Пухова НАН України та проведення експериментів з системою програмування реконфігуровних засобів на базі гріду та хмарної інфраструктури» №0120U103624 (2020 р.), згідно Програми інформатизації НАН України на 2020 р. Більшість з перерахованих НДР було виконано в якості наукового керівника, інші – в якості відповідального виконавця.

Також частка досліджень виконувалась в рамках: Науково-технічної програми «Розвиток системи технічного захисту інформації в Україні», Постанова Кабінету Міністрів України від 21.06.2000 р. №681-009 та програми робіт з організації, стандартизації та сертифікації в галузі ТЗІ, це роботи, які проводились разом з КПІ в інтересах Державної служби спеціального зв’язку та захисту інформації України НДР «РизикМ» договір №239-01 від 15.09.2001р., (2001р.-2007р.).

Результати дисертаційної роботи також застосовувалися при проведенні практичних робіт з експертизи технічних систем захисту. Прикладом таких робіт

є: експертиза «Комутатор зв'язку КС ТУ У 31016953.001-2000» виробництва ЗАТ «Теком», яка виконувалась за дорученням ДСТСЗІ СБ України Інститутом проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України договір №241-03 від 26.12.2003р. «Державна експертиза комплексної системи захисту інформації українського академічного грід-вузла Інституту теоретичної фізики НАН України та комплексної системи захисту інформації Центру реєстрації віртуальних організацій» договір №201-13 від 14.06.13р. «Державної експертиза комплексної системи захисту інформації в автоматизованій системі управління персоналом "Кадри" рівня Укрзалізниці» договір №202-13 від 30.08.13р. «Державна експертиза комплексної системи захисту інформації автоматизованої інформаційної системи Президії Національної академії наук України» договір №203-14 від 22.07.14р. «Державна експертиза комплексної системи захисту інформації локальної обчислювальної мережі Управління справами НАН України» договір №207-16 від 30.06.16р. «Державна експертиза комплексної системи захисту інформації Національного Ресурсного центру Інституту кібернетики НАН України ім. В.М. Глушкова» №208-16 від 30.06.16р. «Державна експертиза комплексної системи захисту інформації на об'єкті, що належить Департаменту військово-технічної політики, розвитку озброєння, та військової техніки Міністерства оборони України» договір №149 від 27.06.18р. «Державна експертиза комплексної системи захисту інформації автоматизованої системи для обробки відкритої інформації Центрального науково-дослідного інституту озброєння та військової техніки Збройних Сил України» договір №211-19 від 17.01.19р.

Мета і завдання дослідження. Метою роботи є забезпечення процесу декомпозиції розмежування доступу до розподілених інформаційних ресурсів, шляхом адаптації системи захисту до поточного стану безпеки кібердовкілля, що обумовлюється вирішенням науково-технічної проблеми породженою об'єктивним протиріччям між існуючою потребою в багатопотоковому доступі до розподілених інформаційних ресурсів грід-систем, з одного боку, та

централізованою однопотоковою архітектурою існуючих засобів захисту, з іншого.

Для досягнення поставленої мети, необхідно розв’язати наступні задачі:

– провести аналіз відомих методів розмежування доступу до ресурсів інформаційних систем та дослідити відповідні математичні моделі з метою виявлення можливостей їх використання для захисту розподілених інформаційних ресурсів;

– удосконалити моделі нейронних мереж для забезпечення керування розмежуванням доступу;

– розробити метод самоорганізації засобів розмежування доступу;

– розробити та дослідити основні інформаційні компоненти розширення функціоналу засобів розмежування доступу до інформаційних ресурсів;

– розробити метод адаптації системи розмежування доступу для розподілених інформаційних ресурсів відповідно до поточного стану безпеки кібердовкілля;

– розробити методи аналізу стану безпеки систем розмежування доступу;

– розробити модель та окремі компоненти засобів системи розмежування доступу;

– провести експериментальні дослідження запропонованих методів, моделей та систем.

Об’єктом дослідження є процес захисту та розмежування доступу до інформаційних ресурсів.

Предметом дослідження є методи і моделі адаптивного захисту та розмежування доступу до ресурсів інформаційних систем.

Методи дослідження. Проведені дослідження базуються на сучасних методах математичного та комп’ютерного моделювання для аналізу отриманих результатів, семантичного аналізу та теорії інформації для побудови структурної моделі засобів інформаційного забезпечення системи розмежування доступу та створення окремих інформаційних компонентів, теорії нейронів та нейронних

мереж, удосконалення структурної моделі нейрона, теорії навчання, самоорганізації та моделювання нейронних мереж для побудови методу самоорганізації засобів розмежування доступу, багатофакторного та системного аналізу для розробки методу адаптації контролю даних в системах розмежування доступу.

Наукова новизна одержаних результатів. В рамках проведених досліджень по вирішенню науково-технічної проблеми одержані наступні основні наукові результати:

– *удосконалено* структурну модель нейрона, в якій за рахунок інтегрування додаткового блоку пам'яті та блоку аналізу, які комутуються до блоку підсумовування вхідних параметрів та формують зворотний зв'язок з функціональними змінними нейрона, реалізується новий функціонал організації контролю даних в системах розмежування доступу;

– *отримав подальший розвиток* метод самоорганізації засобів розмежування доступу, в якому за рахунок застосування правила Хебба та відповідної модифікації адаптаційної залежності, для випадку формування вхідних сигналів, які не містять постійної складової, сформовано співвідношення для побудови рекурентного алгоритму на базі односпрямованої нейронної мережі;

– *вперше розроблено* структурну модель засобів інформаційного забезпечення системи розмежування доступу, в якій за рахунок сюр'єкції множин ідентифікаторів предметних областей користувачів та об'єктів доступу формуються бієкції та набір семантичних правил, що узагальнює процес вирішення завдання побудови взаємозворотних перетворень;

– *вперше запропоновано* метод адаптації системи розмежування доступу, в якому за рахунок генерування зміни оцінки значень параметрів та регулювання їх кількості при збереженні логіки аналізу, система розмежування доступу набуває нового функціоналу автоматичного інкременту або декременту кількості механізмів захисту при відповідній варіабельності стану безпеки ресурсів інформаційних систем;

– *удосконалено* метод аналізу системи розмежування доступу, який за рахунок консолідації оцінок рівня захищеності індивідуальних елементів об’єкта доступу, множини загроз, множини зв’язків із зовнішнім оточенням, функціонального завантаження об’єкта доступу та параметру навантаження обчислювальних ресурсів дозволив отримати комплексну оцінку стану безпеки;

– *вперше розроблено* структурно-функціональну декомпозиційну модель системи розмежування доступу, яка за рахунок блоків аналізу результатів реалізованого доступу, аналізу ситуації відмови в доступі, критеріїв адаптації засобів захисту відповідно до поточного стану безпеки кібердовкілля та керування засобами захисту системи доступу, дозволяє реалізувати запропонований метод адаптації системи розмежування доступу, шляхом розробки та рекомбінації окремих компонентів системи розмежування доступу до розподілених інформаційних ресурсів.

Практичне значення одержаних результатів. Розроблені в роботі моделі та методи адаптації засобів захисту, використовувались при реалізації систем контролю доступу, окремих механізмів захисту та побудові моделей загроз та порушника, а також програм та методик випробувань при проведенні державних експертиз комплексних систем захисту за дорученням ДССЗЗІ СБУ України.

Практична цінність одержаних результатів полягає у такому:

1. Розроблено програми та методики випробувань при проведенні державних експертиз комплексних систем захисту інформації: Центру реєстрації віртуальних організацій української національної грід-інфраструктури Київського національного університету імені Тараса Шевченка, Українського академічного грід-вузла Інституту теоретичної фізики ім. М.М. Боголюбова Національної академії наук України, автоматизованої інформаційної системи Президії Національної академії наук України, автоматизованої системи класу «2» Ресурсного центру Інституту кібернетики Національної академії наук України, локальної обчислювальної мережі Управління справами Національної академії наук України, автоматизованої системи класу «2» для підготовки даних Департаменту військово-технічної політики, розвитку озброєння та військової

техніки Міністерства оборони України, автоматизованої системи для обробки відкритої інформації Центрального науково-дослідного інституту озброєння та військової техніки Збройних Сил України, що підтверджується атестатами відповідності: №9435 від 13.12.2013 р., №9434 від 13.12.2013 р., №11800 від 29.12.2014 р., №14680 від 29.12.2016 р., №14757 від 27.01.2017 р., №17407 від 07.09.2018 р., №19159 від 08.05.2019 р.

2. Модифіковано алгоритми використання ресурсів мережевої інфраструктури на базі проміжного програмного забезпечення Nordugrid ARC, яке є базовим для Українського національного гріду, що підтверджується листом Lund University Department of Physics, Sweden від 06.03.2019.

3. Розроблено грід-сервіс віддаленого синтезу конфігурацій для реконфігуровних засобів захисту інформації Security Tasks Reconfigurable Accelerators Grid-Service на базі гріду та хмарної інфраструктури Українського національного гріду, що підтверджується актом від 28.12.2019 р. по договору №213-19 від 29.03.2019р.

4. Розроблено апаратно-програмний комплекс підтримки прийняття рішень при проведенні державних експертиз комплексних систем захисту інформації, Патент UA 139730 U; G06F17/27. Патент опубліковано 10.01.2020, бюл. № 1.

5. Розроблено апаратно-програмний комплекс моніторингу та керування технологічним процесом зневоднення бішофіту, Патент UA 140326 U; G05B15/00, G05B19/00. Патент опубліковано 10.02.2020, Бюл. № 3.

6. Розроблені в дисертаційній роботі методи побудови засобів захисту на основі використання математичних моделей використовувались в науково-дослідних роботах, що проводились в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України за темами «Кріт», «МодА», «МодБ», «МодД», «Управление», «Модель» та виконувались у відповідності з замовленням Президії академії наук України, а також у роботах за цільовими комплексними програмами відповідно до договорів №200-12 від 30.03.2012р., №200-13 від 01.03.2013р., №205-15 від 06.04.2015р., №206-16 від 15.04.2016р., №210-18 від 16.04.2018р., №213-19 від 29.03.2019р., №213-20 від 15.05.2020р., що

підтверджується звітами виконаних робіт: №0101U006700 від 31.12.2004р., №0105U001296 від 31.12.2008р., №0108U010588 від 31.12.2013р., №0114U002361 від 31.12.2018р., №0102U005589 від 29.12.2006, №0107U001945 від 31.12.2009р., №0112U004018 від 25.12.2012р., №0113U002457 від 25.12.2013р. №0115U002876 від 31.12.2015, №0116U006907 від 31.12.2016р., №0118U001370 від 28.12.2018р., №0119U001812 від 28.12.2019р., №0119U001812 від 28.12.2020р.

7. Результати дисертації впроваджено у діяльність Інституту кібернетики імені В.М. Глушкова Національної академії наук України, ТОВ «Софтлайн ІТ», НДЦ «Нафтогазбурмаш», Департаменту військово-технічної політики, розвитку озброєння та військової техніки Міністерства оборони України, Центральному науково-дослідному інституту озброєння та військової техніки Збройних Сил України, а також використовувалась в навчальному процесі Київського національного університету імені Тараса Шевченка, Національного авіаційного університету для підвищення підготовки фахівців з КБ, що підтверджується актами впровадження: від 19.12.2017р., від 03.12.2018р., від 16.12.2019р., 30.12.2019р., від 05.11.2019р., від 02.08.2017р.

Апробація результатів дисертації. Основні положення дисертаційної роботи доповідались та обговорювались на конференціях та на науково-методичному семінарі, серед яких: V міжнародна науково-практична конференція «Безпека інформації в інформаційно-телекомунікаційних системах» (Київ, 2002), XXII, XXIII, XXIV, XXV, XXVII, XXVIII, XXIX, XXX, XXXI щорічні науково-технічні конференції «Моделювання» (Київ, 2003, 2004, 2005, 2006, 2008, 2009, 2010, 2011, 2012), XXXIII та XXXIV науково-технічні конференції молодих вчених і спеціалістів «Моделювання» (Київ, 2014, 2015), Міжнародна конференція «Информационные технологии в управлении энергетическими системами» (Київ, 2005), VII Всеукраїнська науково-практична конференція рятувальників «Пожежна безпека та аварійно-рятувальна справа: стан, проблеми і перспективи» (Київ, 2005), Науково-практичні конференції «Захист в інформаційно-комунікаційних системах» (Київ, 2006, 2008), пятая международная научно-техническа конференция «Проблемы информатики и моделирования» (Харьков,

2005), Третя Міжнародна наукова молодіжна школа «Высокопроизводительные вычислительные системы» (Таганрог, 2006), Сьома Міжнародна науково-технічна конференція «Искусственный интеллект. Интеллектуальные и многопроцессорные системы» (Таганрог, 2006), Науково-практична конференція «Інтелектуальні системи прийняття рішень та прикладні аспекти інформаційних технологій» (Херсон, 2007), Науково-методичний семінар «Декларування безпеки об'єктів підвищеної небезпеки як засіб регулювання безпеки регіону (держави)» у рамках VI міжнародного виставкового форуму «Технології захисту – 2007» (Київ, 2007), 11-та Всеукраїнська науково-практична конференція «Організація управління в надзвичайних ситуаціях» (Київ, 2009), II, III, XII Міжнародні науково-технічні конференції «Комп'ютерні системи та мережні технології (CSNT)» (Київ, 2009, 2010, 2019), 3-я международная научно-техническая конференция «Моделирование и компьютерная графика - 2009» (Донецк, 2009), International scientific and practical conference «Economics, science, education: integration and synergy» (Bratislava, Slovak Republic, 2016), International scientific and practical conference «Problems and perspectives in European education development» (Prague, Czech Republic, 2016), Annual NorduGrid Conference 2017 (Tromsø, Norway, 2017), III, V, VI Міжнародні науково-практичні конференції «Актуальні питання забезпечення кібербезпеки та захисту інформації» (Київ, 2017, 2019, 2020), The Second International Conference on Computer Science, Engineering and Education Applications (ICCSEEA2019) (Kiev, 2019), Conférence scientifique et pratique internationale «La science et la technologie à l'ère de la société de l'information» (Bordeaux, France, 2019), IX та X Міжнародні науково-технічні конференції «ITSec: Безпека інформаційних технологій» (Київ, Україна; Шарм-ель-Шейх, Египет, 2019, 2020), X Всеукраїнська науково-практична конференція «Актуальні проблеми управління інформаційною безпекою держави» (Київ, 2019), VII Міжнародна науково-технічна конференція «Захист інформації і безпека інформаційних систем». (Львів, 2019), Науково-практична конференція «Кібербезпека енергетики» (Одеса, 2019), XI та XII Всеукраїнські науково-практичні конференції «Стан та удосконалення безпеки інформаційно-

телекомунікаційних систем (SITS)» (Коблево, 2019, 2020), V Всеукраїнська науково-практична конференція «Перспективні напрями захисту інформації 2019» (Затока, 2019), Науково-практичної конференції «Безпека енергетики в епоху цифрової трансформації» (Київ, 2019), Республиканская научно-практическая конференция «Цифровые технологии в промышленности» (Актау, Казахстан, 2019), 1st International Conference on Cyber Hygiene and Conflict Management in Global Information Networks (CyberConf 2019) (Kyiv, 2019), а також наукових семінарах, які проводяться в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України.

Публікації. Базові положення дисертаційного дослідження опубліковані в 175 наукових роботах, основні 57 з яких приведені в авторефераті, в тому числі: 1 монографія [1], 4 наукові праці у міжнародних рецензованих виданнях, що входять до бази даних Scopus [2-5], 2 наукові статі у закордонних фахових наукових журналах (зокрема 1 – без співавторів [6]) [6-7], 7 наукових статей у вітчизняних наукових журналах, які входять в інші міжнародні наукометричні бази даних [8-14], 26 статі у наукових фахових журналах та збірниках (зокрема 15 – без співавторів [15-20, 22-25, 27-29, 34, 36]) [15-40], 2 патенти України [41-42], а також в 15 матеріалів та тез доповідей конференцій (зокрема 2 – без співавторів [45, 46]) [43–57].

Особистий внесок автора. Всі основні положення та результати дисертаційної роботи, що виносяться на захист, отримані автором самостійно. У роботах, написаних у співавторстві, автору належать: [1] – дослідження захисту інформації в авіаційних комп’ютерних мережах; [2] – доведення можливості побудови систем базисних функцій на основі простих розрядних функцій та дослідження властивостей отриманих систем базисних функцій; [3] – дослідження техніки побудови повних ортонормованих систем порозрядних функцій в різних базисах; [4, 7, 10, 26, 48, 49] – основна ідея та постановка задач дослідження, визначення основних етапів методів автентифікації користувачів ІС за клавіатурним та рукописним почерком та множини параметрів, що аналізуються, дослідження доцільності використання нейронних мереж в якості математичного

апарату для вирішення поставленої задачі; [5, 33] – постановка задач дослідження, аналіз впливу множини критичних параметрів та етапів попередньої обробки зразків клавіатурного та рукописного почерку на імовірність правильного розпізнавання користувачів біометричною системою автентифікації; [8] – постановка задач дослідження, аналіз параметрів, що впливають на вибір формальних засобів опису процесів надання повноважень; [9, 38, 50] – постановка задач дослідження, на основі проведених експериментальних досліджень, обґрунтування доцільності застосування запропонованого принципу централізованого синтезу реконфігуровних пристроїв з використанням грід-обчислень для вирішення задач інформаційної безпеки; [11] – основна ідея дослідження, розробка декомпозиційної моделі представлення даних для реалізації експертиз у сфері ТЗІ, формування множин даних; [12, 13, 55, 56] – постановка задач дослідження, формування критеріїв та множини величин, необхідних для реалізації процесу ідентифікації функціонального профілю захищеності в КС, дослідження доцільності використання методу ідентифікації функціонального профілю захищеності для автоматизації процесу генерування функціонального профілю захисту; [14, 57] – постановка задач дослідження, розробка структурної моделі системи підтримки прийняття рішень для реалізації експертиз КСЗІ та формування множини необхідних даних; [21] – аналіз методологій аналізу ризиків при забезпеченні інформаційної безпеки КС; [30-32] – дослідження особливостей використання нейронних мереж для вирішення задач захисту інформації; [35] – основна ідея дослідження, розробка методики проведення експертизи КСЗІ; [37] – постановка задач дослідження, доведення доцільності використання дворівневої моделі доступу до даних при вирішенні прикладних задач; [39] – аналіз структурних підходів оцінки рівня безпеки ІС, які використовують дерево подій та дерево несправностей; [40] – постановка задач дослідження, формування та дослідження множини особливостей взаємозв’язку між процесами, що реалізуються в ІС та процесами, що функціонують в предметній області інтерпретації, яку обслуговує дана система; [41, 42] – розробка схем та алгоритмів функціонування запропонованих апаратно-програмних

комплексів; [43] – розробка методики проектування профілів, адаптивних загрозам за підкласами АС; [44] – постановка задач дослідження, розробка та аналіз основних принципів тестування для аналізу інформаційної безпеки грід-інфраструктур; [47] – дослідження можливості вирішення задач синтезу ПЛІС з використанням ресурсів мережевої інфраструктури на базі проміжного програмного забезпечення Nordugrid ARC; [51, 52] – постановка задач дослідження, аналіз доцільності використання характеристик клавіатурного почерку працівників для реалізації функції моніторингу їх стану; [53] – реалізація багаторівневої моделі доступу та дослідження доцільності її застосування; [54] – розробка підсистем для захисту систем доступу до інформаційних об'єктів енергетики. З робіт, опублікованих у співавторстві, для вирішення проблеми та задач, поставлених у дисертаційному досліджені, використовуються результати отримані особисто здобувачем наукового ступеня.

Структура та обсяг дисертації. Дисертаційна робота складається з анотації, переліку умовних скорочень, вступу, шести розділів, висновків, списку використаних джерел та двох додатків. Дисертація містить 37 рисунків, 3 таблиці. Список використаних джерел складається з 220 найменувань і займає 22 сторінки. Додатки розміщені на 32 сторінках. Загальний обсяг дисертації складає 347 сторінок, основний текст роботи викладено на 262 сторінках.

РОЗДІЛ 1. АНАЛІЗ ПОТОЧНОГО СТАНУ МЕТОДІВ ТА МОДЕЛЕЙ РОЗМЕЖУВАННЯ ДОСТУПУ ДО РЕСУРСІВ ІНФОРМАЦІЙНИХ СИСТЕМ

Нестримний розвиток засобів високопродуктивних обчислень породив багато варіантів обчислювальних архітектур і технологій, прикладом яких є суперкомп'ютери такі як Tianhe-2, Titan – Cray XK7, Sequoia – Blue Gene/Q, K Computer, Mira – Blue Gene/Q та багато інших. Більшість цих комп'ютерів об'єднує масово-паралельна архітектура яка побудована із множині процесорів зв'язаних в єдину обчислювальну мережу. Для звичайних користувачів більш доступні хмарні та грід мережі, експлуатація яких не потребує бюджету супердержави. Якщо суперкомп'ютер це місто в якому замість хмарочосів стоять стойки з електронікою, то грід система це одна вулиця, яка об'єднує приблизно 1000 процесорів поєднаних в три - чотири стойки або взагалі будинок з 24 обчислювальних нод.

Основною перевагою грід систем є можливість об'єднання ресурсів для вирішення ресурсномістких обчислювальних завдань, що мають виконуватися нерегулярно [1-10]. При цьому існує протиріччя між бажанням отримати максимальну продуктивність і необхідністю забезпечення інформаційної безпеки. Проаналізуємо сучасний стан даної проблеми з метою визначення актуальних шляхів її вирішення [11-22]. Грід-системи першого покоління створювалися переважно на принципах довіри один одному та адміністративними одиницями - дослідними лабораторіями та академічними інститутами. Globus Alliance (міжнародний консорціум дослідників грід) разом з іншими науковими і комерційними організаціями працював на основі Open Grid Services Architecture (OGSA). Ця архітектура [23-30] визначає механізми для створення, найменування і пошуку файлів на основі грід-служб.

1.1. Аналіз топології інформаційної безпеки Українського національного гріду

Архітектура захисту інформації в грід-службах забезпечує виконання широкого колу завдань безпеки – від випадків в яких вимоги до захисту мінімальні або зовсім не має, до задач з високого рівня вимогами до забезпечення конфіденційності, цілісності та доступності.

Грід-служби об'єднують різні адміністративні домени, в кожному з яких є особистий автономний механізм захисту. Архітектура безпеки забезпечує протоколи, що дозволяють компенсувати відмінності між автономними механізмами, і при цьому надає кожному локальному вузлу повний контроль над ресурсами, які відносяться до нього.

Загальним для засобів безпеки грід систем є принципи захисту [1, 23]:

1. Автентифікація - надання способу підключення різних механізмів автентифікації і методу їх використання в різних ситуаціях.

2. Передача прав - надання засобів, що дозволяють здійснювати передачу прав доступу від запитуючої сторони до служби, що викликається.

3. Одноразовий вхід - звільнення суб'єктів, які виконали процедуру автентифікації, від необхідності її повторення при кожній спробі доступу до ресурсів на деякий час.

4. Життєвий цикл мандатів і його оновлення - у багатьох випадках можлива ситуація, коли процес, ініційований суб'єктом, виконується довше, ніж час дії виданого мандата. Тому необхідно попередження про це суб'єкта або передбачити оновлення мандата, для того щоб робота могла бути закінчена.

5. Авторизація - дозвіл доступу до служб на підставі політик авторизації, пов'язаних з ними (хто і на яких підставах може здійснювати доступ), і надання можливості стороні, що викликає, задавати політики виконання (кому клієнт довіряє виконання).

6. Конфіденційність - запобігання витоку (розголошенню) будь-якої інформації.

7. Цілісність даних - забезпечення виявлення несанкціонованих змін.

8. Обмін політиками - надання можливості обміну інформацією про політику безпеки сторін, що викликає і викликана, для створення безпечного середовища обміну інформацією.

9. Рівень забезпечення безпеки - реалізація засобів, що дозволяють визначити необхідний рівень забезпечення безпеки системи.

10. Проникність мережевих екранів (firewalls) - основним бар'єром при передачі даних в динамічних, кросдоменних Grid - систем є міжмережеві екрани, тому при проектуванні системи необхідно забезпечити можливість вільної передачі даних через екран без зміни їх політик безпеки.

Більшість з перерахованих вище принципів увійшли в стандарт під назвою OGSA (Security Architecture for Open Grid Services), розроблений Open Grid Forum (OGF), і на сьогоднішній день Globus Toolkit (GT) є широко поширеною реалізацією цього стандарту.

Апаратною базою реалізації дослідження було обрано елементі Українського національного гріду (УНГ), тому розглянемо топологію організації інформаційної безпеки внутрішнього.

Основними елементами УНГ є [1-7]:

— ресурсні центри національного рівня;

— Центр сертифікації з регіональними філіями;

— Центр реєстрації віртуальних організації;

— Центр моніторингу грід-інфраструктури та реєстрації грід-сайтів;

— грід-сайти - вузли УНГ, що підключені до національної грід-інфраструктури.

Координацію роботи для підтримки, функціонування УНГ проводить Базовий координаційний грід-центр Українського національного гріду і регіональні координаційні грід-центри.

Автентифікація в грід-системі реалізована з використанням програмного продукту NorduGrid [8, 27] і використовує сертифікат відкритого ключа X.509 [3] інфраструктури відкритих ключів [4]. Типова схема взаємодії між користувачем і кластером в грід-середовищі наведена на рис. 1.1.1. В процесе реалізації

санкціонованого доступу проміжне програмне забезпечення NorduGrid від імені автентифікованого користувача запускає на ідентифікованому кластері розподілений програмний застосунок користувача (РППЗ). Зазвичай РППЗ використовує інтерфейс передавання повідомлень Message Passing Interface (MPI) [5] для організації обміну повідомленнями в розподіленому середовищі, а конкретний екземпляр РППЗ виконується в операційної системі (ОС) конкретного обчислювального вузла. Схемі взаємодії РППЗ, NorduGrid і MPI мають високу динаміку змін, тому для них необхідне динамічне формування вимог безпеки. З іншого боку, операційні та мережеві середовища мають традиційні функції і складають основу безпеки, для них існують типові вимоги, оскільки від них залежить безпека функціонування грід-середовища в цілому зазвичай з них формується політика безпеки. Але це породжує протиріччя між звичайними однопотоковими механізмами захисту інформації та паралельним середовищем основою якого є архітектура MPI.

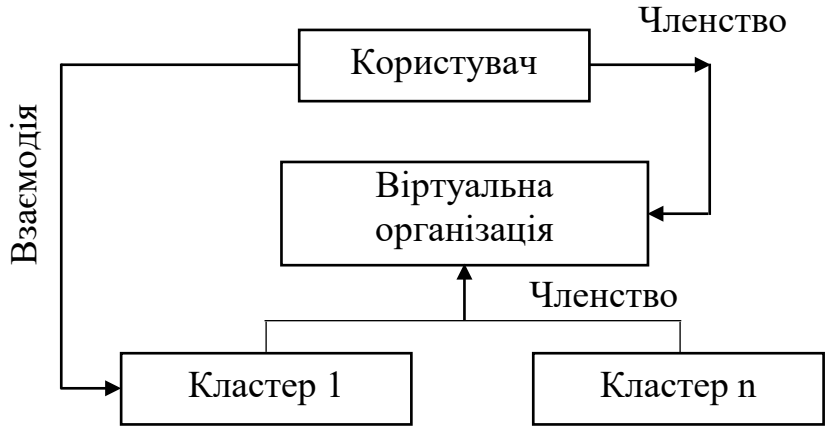


Рисунок 1.1.1 – Типова взаємодія в грід-середовищі

Актуальною версією проміжного програмного забезпечення (ППЗ) ARC [9, 12, 25] в УНГ (див. рис. 1.1.2) на початок 2021 року є версія 5.0.2. Розглянемо його реалізацію, а саме підсистемі які є його складовими. Це є наступні грід-служби: Керування завантаженням; Керування даними; Інформаційне забезпечення; Безпека і контроль прав доступу; Протоколювання; Обчислювальний елемент.

Підсистема *керування завантаженням* Workload Management System (WMS) здійснює розподіл завдань за допомогою брокера (планувальника) завдань, визначає, який ресурс зараз вільний, і стежить за виконанням завдань, здійснює фактичні операції з управління завданнями: спрямовує на виконання, вилучає, і т.д., формує відповідне середовище для виконання на робочому вузлу кластера.

Підсистема *керування даними* Data Management System (MD) забезпечує функціонування глобальної файлової системі в масштабах всієї грід-інфраструктури. Вона складається з трьох сервісів, що підтримують доступ до файлів:

— сервіс зберігання даних Storage Element (SE) - сукупність служб, необхідних для забезпечення доступу до файлів, що зберігаються на сайті;

— сервіс каталогів Catalog Services (CS);

— брокер передачі даних Data Scheduler (DS).

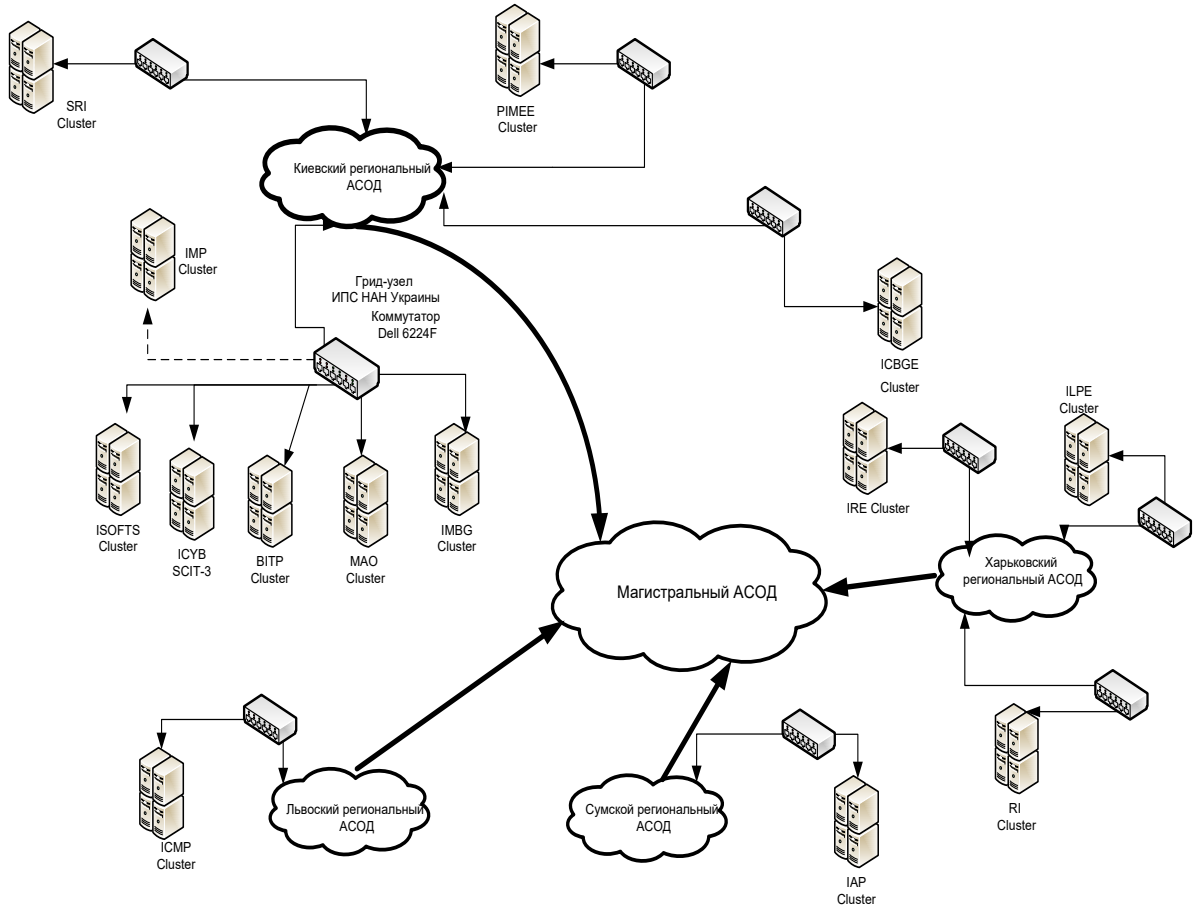


Рисунок 1.1.2 – Інфраструктура академічного гріду

Підсистема *інформаційного забезпечення* Information System (IS) і *моніторингу грід-системи* Relational Grid Monitoring Architecture (R-GMA) вирішує задачу збору та управління даними про стан грід-інфраструктури, збираючи інформацію від розподілених постачальників – першоджерел інформації. Призначена для постійного контролю функціонування грід-інфраструктури та забезпечення своєчасного реагування на проблеми під час їх виникнення.

Підсистема *безпеки і контролю прав доступу* Grid Security Infrastructure (GSI) забезпечує безпечний доступ до ресурсів грід-сайту з урахуванням прав користувача і правил обслуговування користувачів (реалізацію «локальної політики»). Підсистема включає сервіси забезпечення:

— *автентифікації* – перевірка достовірності об'єкта (користувача або грід-вузла), що направив запит на виконання якої-небудь дії;

— *авторизації* – зіставлення об'єкта і набору прав (привілеїв) при роботі в грід-інфраструктурі;

— *конфіденційності передачі інформації* – доступність даних, що передаються тільки заздалегідь обумовленому набору об'єктів;

— *цілісності передачі інформації* – незмінність переданих даних;

— *делегування прав* (мається на увазі, що користувачеві потрібно лише один раз пройти процедуру автентифікації, а далі система сама забезпечить його ідентифікацію на всіх ресурсах, які він планує використовувати).

Підсистема *протоколювання* Logging and Bookkeeping (LB) відстежує які грід-кроки обробки завдання виконуються в різних точках системи, фіксуючи і запам'ятовуючи події, що відбуваються, наприклад - запуск, визначення на якому конкретно обчислювальному елементу буде виконано поточне завдання, початок виконання і т.д.

Підсистема *обчислювальних елементів* Computing Element (CE) об'єднує обчислювальні ресурси сайту і виконує функції управління завданнями (запуск, видалення і т.д.), а також генерує інформацію про стан ресурсів.

Основою для побудові політики безпеки грід-сайту є визначення:

1. Відповідальних осіб за встановлення правил доступу;
2. Складу інформації, що підлягає захисту;
3. Типів користувачів/груп користувачів, для яких надаються права доступу;
4. Множині санкціонованих прав доступу;
5. Основних правил надання доступу.

Зазвичай відповідальними особами є *адміністратор (менеджер) віртуальної організації*, до якої належить користувач, та *адміністратор безпеки грід-сайту* - власника ресурсів.

Кожна віртуальна організація (ВО) самостійно встановлює правила роботи для своїх учасників, виходячи з дотримання балансу між потребами користувачів і наявним обсягом ресурсів, тому користувач повинен обґрунтувати свої потреби в ресурсах грід-системі і отримати згоду керуючих органів ВО.

Для гнучкого управління правами різних користувачів віртуальна організація може визначити групи користувачів з різними правами, а користувачам можуть бути приписані окремі ролі. Цим групам і користувачам в процесі авторизації визначаються різні права доступу до грід-сервісів.

До інформації, доступ до якої підлягає обмеженню, належить:

— інформація користувачів;
— технологічна інформація.

Програмне забезпечення, призначене для обробки і захисту цієї інформації:

— прикладні застосунки користувачів;
— ППЗ, яке бере участь в обробці інформації;
— програмне забезпечення з управління грід-інфраструктурою;
— засоби захисту інформації.

За рівнем повноважень щодо доступу до інформації, пов’язаної з характером і складом робіт в грід-сайті виділяються наступні категорії:

— користувач грід-сайту;
— групи користувачів (з однаковими правами);
— адміністратори грід-сайту.

Для кожної категорії встановлюються повноваження щодо доступу до файлів і директорій глобального грід-каталогу, файлів і директорій ОС грід-сайту. Відповідно до політики яка зазвичай реалізована в ОС ARC і gLite користувач має право працювати з файлами тільки на рівні не вище директорії, яка була створена для даного ПЗ.

В якості ідентифікаторів користувачів і ресурсів в GSI використовуються цифрові сертифікати стандарту X.509 (стандарт міжнародної організації International Telecommunication Union, ITU).

Вимоги щодо забезпечення інформаційної безпеки в гріду можна згрупувати в чотири множини. Це вимоги до автентифікації, управління обліковими записами користувачів, реагування на інциденти безпеки та моніторингу. Забезпечення цих вимог потребує певних механізмів захисту.

Механізми автентифікації для грід-сайту повинні забезпечувати:

— **єдиний вхід** – користувач повинен зареєструватися і автентифікуватися тільки один раз на початку сеансу роботи, отримуючи доступ до всіх санкціонованих ресурсів ґрід - сайту;

— **делегування прав** – користувач повинен мати можливість запуску власних програм від свого імені. Має бути забезпечено доступ програми до всіх ресурсів санкціонованих для користувачу. Особисті програми можуть, при необхідності, делегувати частину своїх прав іншим програмам.

Механізми управління обліковими записами користувачів для грід-сайту повинні забезпечувати:

— **контроль унікальності ідентифікатору та паролю** (атрибуту) в рамках операційної системи грід-сайту на підставі відповідного сертифіката користувача;

— **контроль за безпекою паролів**, яка включає перевірки якості процедур генерування та збереження;

— **блокування** облікових записів;

— **реєстрацію** дій по створенню, модифікації та віддаленню облікових записів.

Механізми реагування на інциденти безпеки для грід-сайту повинні забезпечувати можливість контролювати небезпечні дії шляхом розпізнавання, фіксації та аналізу дій і подій, пов’язаних з дотриманням політики безпеки інформації.

Механізми моніторингу для грід-сайту повинні забезпечувати [28-30]:

— функціонування **журналів реєстрації дій** адміністраторів і користувачів, а також неполадок, що виникають в процесі обробки інформації.

— **перевірку** вжитих заходів і **верифікацію** їх відповідності політиці доступу.

— **збереження** протягом погодженого періоду журналу аудиту, для сприяння в майбутніх розслідуваннях і моніторингу контролю доступу.

— **контроль за переглядом** на регулярній основі журналів реєстрації адміністраторами грід-сайту.

— **захист інформації та засобів її реєстрації** від фальсифікації та несанкціонованого доступу.

Таблиця 1.1.1

Продуктивність кластерів УНГ

№	Установа	Місто	Грід-сайт	Кіль. ядер	Частота, МГц	Процесори	Пікова продук., Гфлоп	ОС
1.	Інститут теоретичної фізики (ИТФ) ім. М.М. Боголюбова НАН України	Київ	BITP Cluster	464	2000	Intel Xeon	**3712**	CentOS Linux 7.7.1908
2.	Навч. центр ИТФ ім. М.М. Боголюбова НАН України	Київ	BITPEDU ARC Cluster	8	2000	Intel Xeon	**640**	Scientific Linux 2.5.58
3.	Національний науковий центр з медико-біотехнічних проблем при Президії НАН України	Київ	CHIMERA	204	2000	Intel Xeon	**1632**	CentOS 7.6
4.	Інститут прикладних проблем механіки і математики ім. Я.С. Підстригача НАН України	Львів	IAPMM Cluster	88	2400	Intel Xeon	**845**	CentOS 5.6
5.	Інститут електронної фізики НАН України	Ужго-род	IEP Cluster	52	2000	Intel Xeon	**416**	Linux-2.6.18-371.4.1.el5
6.	Інститут харчової біотехнології та геноміки НАН України	Київ	IFBG Cluster	60	3200	Intel Xeon	**768**	Scientific Linux 6.10

Закінчення таблиці 1.1.1

№	Установа	Місто	Грід-сайт	Кіль. ядер	Частота, МГц	Процесори	Пікова продук., Гфлоп	ОС
7.	Фізико-технічний інститут низьких температур ім. Б.І. Вєркіна НАН України	Харків	ILTPE Cluster	56	2270	Intel Xeon	**508**	CentOS 6.10 Carbon
8.	Інститут математики НАН України	Київ	IMATH Cluster	24	1860	Intel Xeon	**179**	н/д
9.	Інституту металофізики ім. Г.В. Курдюмова НАН України	Київ	IMP ARC	80	1860	Intel Xeon	**595**	Scientific Linux 5.x
10.	Інститут проблем матеріалознавства ім. І.М. Францевича НАН України	Київ	IPMS Cluster	32	1800	Intel Atom	**115**	CentOS 7.5
11.	Інститут радіофізики та електроніки ім. О.Я. Усикова НАН України	Харків	IRE Cluster	64	2270	Intel Xeon	**581**	Scientific Linux 6.3 Carbon
12.	Інститут сцинтиляційних матеріалів НАН України	Харків	ISMA cluster	220	2660	Intel Xeon	**2341**	CentOS 7.6
13.	Київський національний університет імені Тараса Шевченка	Київ	KNU ARC-6	240	2000	Intel Xeon	**1920**	CentOS 7.9
15.	Державний науково-дослідний інститут автоматизованих систем в будівництві	Київ	NDIASB cluster	2	2000	Intel Xeon	**16**	CentOS 7.1
16.	Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України	Київ	PIMEE ARC	24	2000	Intel Xeon	**192**	Scientific Linux 6.3

В подальшому, по мірі необхідності, буде розглянуто їх реалізацію для потрібних конфігурації апаратних та програмних засобів.

Таким чином нами розглянуто топологію інформаційної безпеки Українського національного гріду який визначено базовим програмно-апаратним засобом на прикладі якого показано функціонал системи безпеки і контролю прав доступу, сформовані множині завдань безпеки та механізмів їх реалізації. Це дозволило показати протиріччя між звичайними однопотоковими механізмами захисту інформації та паралельним середовищем основою якого є архітектура MPI, що застосується для реалізації процедур розпаралелювання в грід-системах.

Оцінемо продуктивність кластерів УНГ (див. табл. 1.1.1). Наведені дані показують істотне зростання пікової продуктивності до 3712 Гфлоп. При мінімальній продуктивності 16 Гфлоп. Для EGI показники будуть ще більше. Збільшення продуктивності веде до збільшення розриву з однопотоковими механізмами захисту.

1.2. Аналіз моделей розмежування доступу до ресурсів інформаційних систем

Моделі розмежування доступу необхідні для побудові політик безпеки спрямованих на забезпечення конфіденційності, цілісності, доступності та спостереженості. Класична класифікація цих моделей [31] передбачає розподіл їх за типами побудові на основі принципів:

- надання прав;
- теорії інформації;
- теорії вірогідності.

В свою чергу моделі розмежування доступу побудовані на основі принципів надання прав розподіляються на моделі дискреційного и мандатного доступу. Найбільш відомі моделі дискреційного типу це модель АДЕПТ-50 [32].

Інша назва цього типу - вибіркове керування доступом (дискреційне керування доступом, контрольоване керування доступом) (англ. Discretionary access control, DAC) - керування доступом суб’єктів до об’єктів на основі списків

керування доступом, які задають однозначну відповідність між об'єктами, суб'єктами і можливими діями (типами доступу, операціями), або на основі матриці доступу. Тобто для кожної пари (суб'єкт - об'єкт) має бути заданий явний і недвозначний перелік санкціонованих типів доступу (читати, писати і т.д.) даного суб'єкта (індивіда або групи індивідів) до даного ресурсу (об'єкту). При запиті на доступ до об'єкта, система шукає суб'єкта в списку прав доступу об'єкта і надає доступ, якщо суб'єкт присутній в списку і дозволений тип доступу включає тип, що вимагається. Інакше доступ не надається.

Моделі DAC реалізуються за допомогою:

— списків контролю доступу;

— ідентифікації суб'єкта.

Формально в моделі DAC відношення "суб'єкти-об'єкти" представляють у вигляді матриці доступу, що має наступну структуру:

— в рядках матриці доступу перераховані об'єкти;

— в стовпцях матриці доступу перераховані суб'єкти;

— в клітинках, розташованих на перетині рядків і стовпців, записані додаткові умови (наприклад, час і місце дії) і дозволені види доступу.

Гнучкість DAC дозволяє використовувати його у великій кількості систем і застосунків. Прикладом використання DAC є системи Windows NT/2k/XP.

Однак у DAC є і **недоліки**:

Відсутність повної гарантії того, що інформація не стане доступна суб'єктам, які не мають до неї доступу. Це проявляється в тому, що суб'єкт, який має право на читання інформації, може передати її іншим суб'єктам, які цього права не мають, без повідомлення власника об'єкта. Система DAC не встановлює ніяких обмежень на поширення інформації після того як суб'єкт її отримав.

Всі об'єкти в системі належать суб'єктам, які налаштовують доступ до них для інших. На практиці виявляється, що в більшості випадків дані в системі не належать окремим суб'єктам, а належать всій системі.

Складність керування доступом (ведення матриці доступу), яка в реальних системах пов'язана:

— з великою розмірністю цієї матриці (великим числом суб’єктів і об’єктів);

— з високим динамізмом її коригування;

— з необхідністю постійного відстеження при таких корегуваннях великого числа залежностей між значеннями певних кортежів. Наявність таких залежностей пов’язано з об’єктивно існуючими в предметній області обмеженнями і правилами успадкування повноважень в ієрархії об’єктів і суб’єктів.

Наприклад, користувач повинен наслідувати повноваження груп користувачів, в які він входить. Права доступу деякого користувача до каталогів і файлів не повинні перевищувати відповідні його права доступу до диска, на якому вони розміщені і т.п.).

При повноважному керуванні доступом (категорування об’єктів та суб’єктів і введення обмежень по доступу встановлених категорій суб’єктів до об’єктів різних категорій) на матрицю доступу накладаються додаткові залежності між значеннями прав доступу суб’єктів.

Обмеження і залежності між повноваженнями істотно ускладнюють процедури ведення матриць доступу. Це призвело до виникнення великої кількості способів неявного завдання матриці (списки доступу, перелік повноважень, атрибутні схеми і т.п.).

Класична система дискреційного контролю доступу називається «закритою» в тому сенсі, що спочатку об’єкт не доступний нікому, і в списку прав доступу описується список дозволів. Також існують «відкриті» системи, в яких за замовчуванням всі мають повний доступ до об’єктів, а в списку доступу описується список обмежень.

Особливістю моделі є необхідність наявності або чітко виділених власників ресурсів, які керують доступом, або суперадміністраторів, що мають досить великі повноваження. У масштабних інфраструктурах застосування моделі ускладнюється швидко зростаючою складністю керування, що проявляється в кількості і розмірі списків керування доступом.

Мандатне керування доступом (англ. Mandatory access control, MAC) – розмежування доступу суб'єктів до об'єктів, засноване на призначенні мітки конфіденційності для інформації, що міститься в об'єктах, і видачу прав суб'єктам на звернення до інформації такого рівня конфіденційності. Цей тип доступу поєднує обмеження прав доступу і захист інформації, які застосовуються по відношенню до комп'ютерних процесів, даних і системних пристроїв і призначені для запобігання їх несанкціонованому використанню.

Мандатна модель керування доступом є основою для реалізації політики розмежування доступу до ресурсів при захисті інформації з обмеженим доступом. Але на практиці дана модель доступу не використовується без доповнення елементами інших моделей доступу. Вона є альтернативою дискреційному контролю доступу і може заміняти або доповнювати його. Найважливіша перевага полягає в адміністративному характері доступу, тобто користувач не може повністю контролювати доступ до ресурсів, які він створює.

Широко використається в сучасних операційних системах, реалізована в ОС FreeBSD, Unix. У SUSE Linux і Ubuntu є архітектура мандатного контролю доступу під назвою AppArmor. Існують також механізми мандатного контексту безпеки, пов'язаного з кожним суб'єктом, і мандатної мітки, пов'язаної з об'єктом в операційних системах спеціального призначення, наприклад Astra Linux Special Edition. В мережеві пакети протоколу IPv4 відповідно до стандарту RFC1108 впроваджуються мандатні мітки, відповідні мітці об'єкта – мережеве з'єднання. У захищених комплексах гіпертекстової обробки даних, електронної пошти і в інших сервісах, мандатне розмежування реалізовано на основі програмного інтерфейсу бібліотек підсистеми безпеки PARSEC. Але всі ці реалізації орієнтовані на однопотокове використання і потребують додаткових зусиль для застосування в розподілених обчислювальних середовищах.

Розглянемо більш детально реалізацію найбільш важливих моделей доступу [33-43].

Модель Бела — ЛаПадули — модель контролю та керування доступом, мета побудові аналіз умов, при яких неможливе утворення інформаційних потоків

від суб'єктів з вищим рівнем доступу до суб'єктів з нижчим рівнем доступу. Класична модель Бела — ЛаПадули описана у 1975 р. співробітниками MITRE Corporation Девідом Белом та Леонардом ЛаПадулою [33][34]. Сутність системи полягає у тому, що кожному суб'єкту і об'єкту надавалась мітка конфіденційності, починаючи з найвищої до найнижчої. Причому суб'єкт, якому дозволено доступ до об'єктів з нижчою міткою конфіденційності, не може отримати доступ до об'єкта з вищою міткою конфіденційності. Також суб'єкту забороняється запис у об'єкти з нижчою міткою конфіденційності. Модель Бела — ЛаПадули описується скінченним автоматом з допустимим набором станів, у яких може знаходитись інформаційна система.

Поняття захищеної визначається наступним чином: кожен стан системи повинен відповідати політиці безпеки, встановленої для даної інформаційної системи. Перехід між станами описується функціями переходу. Система знаходиться у безпечному стані тільки у тому випадку, коли у кожного суб'єкта наявний доступ тільки до тих об'єктів, до яких від дозволений на основі поточної політики безпеки. Для визначення права доступу суб'єкта до об'єкта рівень доступу суб'єкта порівнюється з рівнем таємності об'єкта, і на підставі цього приймається рішення щодо надання запитаного рівня доступу. Набори рівень доступу/рівень таємності описуються матрицею доступу. Формально ця модель описана як :

— S – множина суб'єктів;

— O – множина об'єктів, $S \subset O$;

— $R = \{r, w\}$ – множина прав доступу, r – доступ на читання, w – доступ на запис;

— $L = \{U, SU, S, TS\}$ – множина рівнів таємності, U – відкрита, SU – для службового користування, S – таємна, TS – цілком таємна;

— $\Lambda = (L, \leq, \bullet, \otimes)$ – решітка рівнів секретності, де:

○ $\leq$ – оператор, що визначає часткове несуворе відношення порядку рівнів таємності;

- $\bullet$ – оператор найменшої верхньої межі;
- $\otimes$– оператор найбільшої нижньої межі.

— V – множина станів системи, що представляється у вигляді впорядкованих пар (F,M), де:

- F:S∪O→L – функція рівнів таємності, яка ставить у відповідність кожному об'єкту і суб'єкту в системі певний рівень таємності;
- M – матриця поточних прав доступу.

Оператор відношення ≤ має наступні властивості:

— Рефлексивність: 8a∈L:a≤a, полягає у тому, що між суб'єктами та об'єктами одного рівня таємності передача інформації дозволена.

— Антисиметричність: ∀a_1, a_2∈L:((a_1≤a_2)&(a_2≤a_1)) → a_2=a_1, полягає у тому, що якщо інформація може передаватися від суб'єктів та об'єктів рівня А до суб'єктів та об'єктів рівня В, і від суб'єктів та об'єктів рівня В до суб'єктів та об'єктів рівня А, то ці рівні еквівалентні.

— Транзитивність: ∀a_1, a_2, a_3∈L:((a_1≤a_2)&(a_2≤a_3)) → a_1≤a_3, полягає у тому, що якщо інформація може передаватися від суб'єктів і об'єктів рівня А до суб'єктів і об'єктів рівня В, і від суб'єктів і об'єктів рівня В до суб'єктів і об'єктів рівня С, то вона може передаватися від суб'єктів і об'єктів рівня А до суб'єктів і об'єктів рівня С.

Оператор найменшої верхньої межі $\bullet$ визначається відношенням:

a=a_1•a_2 ⇔ (a_1, a_2≤a) & (∀a'2L:(a'≤a) → (a'≤a_1∨a'≤a_2)).

Оператор найбільшої нижньої межі $\otimes$ визначається відношенням:

a=a_1⊗a_2 ⇔ (a≤a_1, a_2) & (∀a'2L:(a'≤a_1&a'≤a_2) → (a'≤a)).

З визначення цих двох операторів можна показати, що для кожної пари a_1, a_2 2L існує єдиний елемент найменшої верхньої межі та єдиний елемент найбільшої нижньої межі.

Система $\Sigma = (v_0, R, T)$ у моделі Бела – ЛаПадули складається з наступних елементів:

v_0 – початковий стан системи;

R – множина прав доступу;

$T : V \times R \rightarrow V$ – функція переходу, яка у ході виконання запитів переводить систему із одного стану у інший.

Визначення безпечного стану:

Стан v називається досяжним у системі $\Sigma = (v_0, R, T)$, якщо існує послідовність $\{(r_0, v_0), ..., (r_{n-1}, v_{n-1}), (r_n, v_n)\}: T(r_i, v_i) = v_i + 1 \forall\ i = 0, n - 1$. Початковий стан v_0 є досяжним за визначенням.

Стан системи (F, M) називається безпечним по читанню (або просто безпечним (від простої властивості)), якщо для кожного суб'єкта, який здійснює у цьому стані доступ на читання до об'єкта, рівень доступу суб'єкта переважає рівень таємності об'єкта:

$\forall s \in S, \forall o \in O, r \in M\ [s,o] \rightarrow F(o) \leq F(s)$

Стан системи (F, M) називається безпечним по запису, якщо для кожного суб'єкта, який здійснює у цьому стані доступ на запис до об'єкта, рівень таємності об'єкта переважає рівень доступу суб'єкта:

$\forall s \in S, \forall o \in O, w \in M\ [s,o] \rightarrow F(s) \leq F(o)$

Стан (F, M) називається безпечним, якщо він є безпечним і по читанню, і по запису.

Система $\Sigma=(v_0, R, T)$ називається безпечною, якщо її початковий стан v_0 є безпечним, і усі стани, які можуть бути досягнуті з v_0 шляхом застосування скінченної послідовності запитів з R, безпечні.

Основна теорема безпеки Бела — ЛаПадули:

Система $\Sigma=(v_0, R, T)$ безпечна тоді, і тільки тоді, коли виконані наступні умови:

– Початковий стан v_0 є безпечним.

– Для будь-якого стану v, який досяжний з v_0 шляхом застосування скінченної послідовності запитів з R, таких, що $T(v,r)=v^*$, $v=(F, M)$ і $v^*=(F^*, M^*)$, для $\forall s \in S, \forall o \in O$ виконані умови:

- Якщо $r \in M^*[s, o]$ і $r \notin M\ [s, o]$, то $F^*(o) \leq F^*(s)$
- Якщо $r \in M\ [s, o]$ і $F^*(s) < F^*(o)$, то $r \notin M^*[s, o]$
- Якщо $w \in M^*[s, o]$ і $w \notin M\ [s, o]$, то $F^*(s) \leq F^*(o)$

- Якщо $w \in M[s, o]$ і $F^*(o) < F^*(s)$, то $w \notin M^*[s, o]$

Крим загально відомих до недоліків цієї моделі в нашому випадку треба віднести централізований характер розмежування доступу, який не враховує можливість розподіленого збереження та обробки даних.

Модель Take-Grant (від англ. take «брати», grant «давати») – це формальна модель, яка використовувана в області комп'ютерної безпеки, для аналізу систем дискреційного розмежування доступу; підтверджує або спростовує ступені захищеності даної автоматизованої системи, яка повинна задовольняти регламентованим вимогам. Модель представляє всю систему як спрямований граф, де вузли – або об'єкти, або суб'єкти. Дуги між ними марковані, і їх значення вказують права, які має об'єкт або суб'єкт (вузол). У моделі домінують два правила: «брати» і «давати». Вони відіграють в ній особливу роль, переписуючи правила, що описують допустимі шляхи зміни графа [45-55]. В цілому існує 4 правила перетворення:

- правило «брати»;
- правило «давати»;
- правило «створити»;
- правило «видалити»;

Використовуючи ці правила, можна відтворити стани, в яких перебуватиме система залежно від розподілу і зміни прав доступу. Отже, можна проаналізувати можливі загрози для даної системи.

Звичайна модель

- O – множина об'єктів (файли, сегменти пам'яті і т. д.);
- S – множина суб'єктів (користувачі, процеси системи);
- $R = \{r_1, r_2, r_3, r_4, \ldots, r_n\} \cup \{t, g\}$ – множина прав доступу;
- t [take] – право брати «права доступу»;
- g [grant] – право давати «права доступу»;
- G = (S, O, E) – скінченний, позначений, орієнтований граф без петель;
- × – об'єкти, елементи множини O;

— • – суб’єкти, елементи множини S;

— E ∈ O x O x R – дуги графа.

Стан системи описується її графом.

Перетворення **G** в граф **G'** = правило і позначається: [$G - opG'$]

Правило «брати»

Брати = take(r, x, y, s), r ∈ R.

Нехай s ∈ S, x,y ∈ O – вершини графа G.

Тоді граф G (див. рис. 1.2.1):

Рисунок 1.2.1 – Правило «брати»

Тобто суб’єкт *S* бере у об’єкта *X* права r на об’єкт *Y*.

Правило «давати»

Давати = grant(r, x, y, s), r ∈ R.

Нехай s ∈ S, x,y ∈ O – вершини графа G.

Тоді граф G (див. рис. 1.2.2):

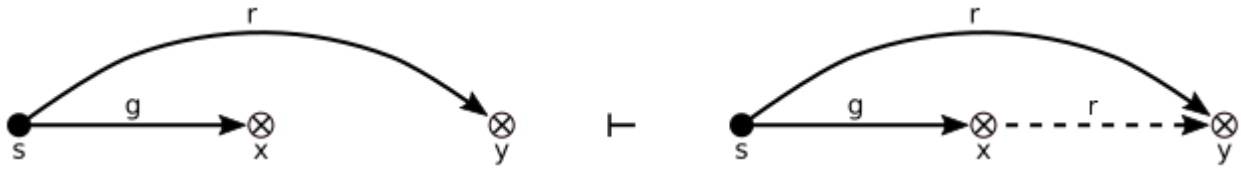


Рисунок 1.2.2 – Правило «давати»

Тобто суб’єкт *S* дає об’єкту *X* права r на об’єкт *Y*.

Правило «створити»

Створити = create(p, x, s), r ∈ R.

Нехай s ∈ S, x,y ∈ O — вершини графа G.

Тоді граф G (див. рис. 1.2.3):

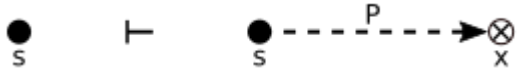


Рисунок 1.2.3 – Правило «створити»

Тобто суб’єкт *S* бере r- доступний об’єкт X.

Правило «видалити»

Видалити = remove(r, x, s), r ∈ R.

Нехай s ∈ S, x,y ∈ O — вершини графа G.

Тоді граф G (див. рис. 1.2.4):

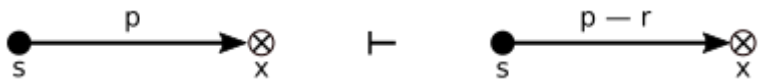


Рисунок 1.2.4 – Правило «видалили»

Приклади реалізації

1. На рисунку 1.2.5 показано графічне представлення структури каталогів. У цьому графі P1 і P2 є суб’єктами (можливі користувачі), а Ds і Fs представляють об’єкти, каталоги і файли, відповідно. Право «читання» було змінено на правило «брати» для всіх рівнів, за винятком фактично файлових рівнів в каталогах. Право «запису» також змінилося правилом «давати». Стає ясно з цього графа: якщо суб’єкт має право читання (брати) об’єкта, то він може мати право на читання будь-яких інших об’єктів, на які цей перший об’єкт має якісь права. Аналогічно, якщо суб’єкт має право запису (давати) об’єкта, він може надати будь-яке з своїх прав на цей об’єкт.

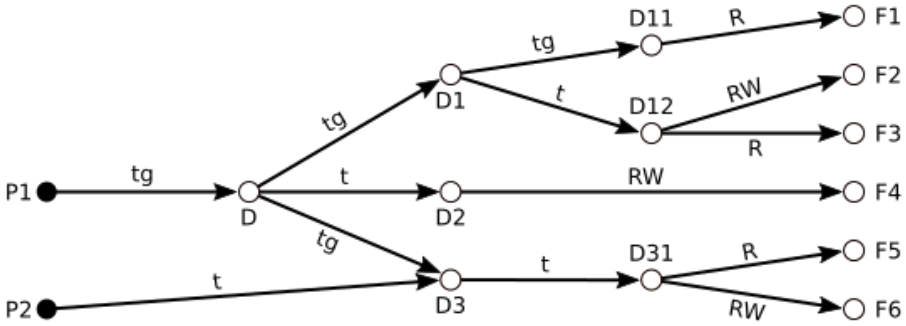


Рисунок 1.2.5 – Графічне представлення структури каталогів

2. На рисунку 1.2.6 показано, що за допомогою комбінації із зазначених вище чотирьох правил, новий файл може бути доданий в каталог структури Прикладу 1. І права на читання/запис, будуть призначені згідно з правилами, що використовуються каталогом, в якій цей файл записується. Наступні чотири

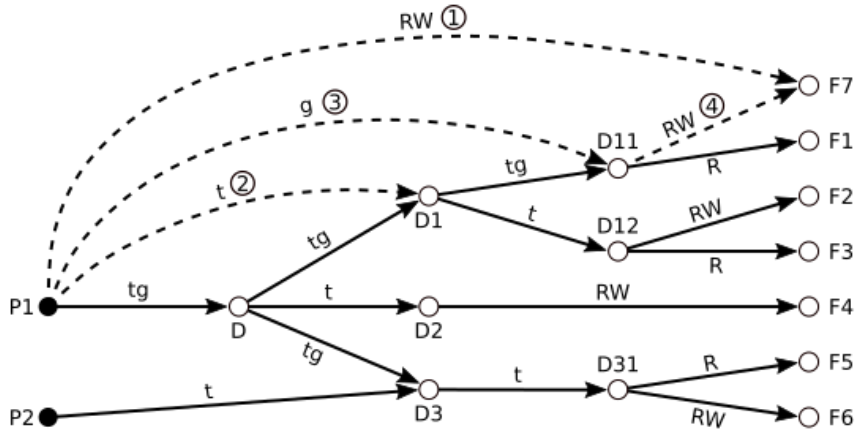


Рисунок 1.2.6 – Демонстрація можливості додавання нового файлу в існуючий каталог структури

кроки необхідні для додавання файлу і дозволу права:

1. P1 створює R/W для нового об’єкта F7;
2. P1 прийняти t для D1 від D;
3. P1 прийняти g для D11 з D1;
4. P1 дарувати RW від F7 до D11.

Номери у списку вище, відповідають обведеним номерам, що зображені на графіку, як створюється дуга графа.

Завдяки формалізації ця модель має великий потенціал але потребує розвитку для розподіленого застосування.

Розмежування доступу на основі атрибутів (англ. *Attribute-Based Access Control, ABAC*) – модель контролю доступу до об’єктів, заснована на аналізі правил для атрибутів об’єктів або суб’єктів, можливих операцій над ними та оточенням, що відповідає запиту [50-60]. Системи управління доступом на основі атрибутів забезпечують мандатне та дискреційне керування доступом.

Головними компонентами будь-якого механізму контролю доступу є автентифікація та ідентифікація користувача. Доступ до мережі інформаційної системі установі або її ресурсів зазвичай залежить від функціональних обов’язків

співробітника. Наприклад, системній адміністратор має можливість доступу до технологічної інформації, менеджер баз даних тільки в частині яка стосується керування базою даних, а користувач взагалі має доступ тільки до окремої частки даних. Якщо співробітник змінює посаду або звільняється, адміністратор повинен вручну поміняти його роль, щоб змінити права доступу, можливо навіть в декількох системах. Для того, щоб в такому і в більш складних випадках спростити процес зміни прав, установі потрібен більш гнучкий підхід до контролю доступу [61-65].

Політика на основі атрибутів робить керування доступом більш ефективним, зменшуючи складність нормативних вимог. Одна і та ж політика, заснована на атрибутах, може використовуватися в різних системах. Це допомагає керувати узгодженістю доступу до ресурсів в межах однієї установі або між декількома її філіями. Таке централізоване керування доступом передбачає єдине джерело для правил доступу, що робить необов'язковими перевірки на відповідність вимогам кожної конкретної системи зі своєю політикою [66-70].

Розвитком моделі ABAC є моделі на основі автентифікації (англ. *autheNtication-Based Access Control, NBAC*) і авторизації (англ. *authoriZation-Based Access Control, ZBAC*), де враховується проблема узгодження значень атрибутів і зменшується кількість міждоменних угод, але при цьому потрібні деякі зміни у початкових системах [71-73].

Вперше контроль доступу був застосований в Міністерстві оборони США в 1960х-1970х роках і включав моделі дискреційного (англ. *Discretionary Access Control, DAC*) і мандатного доступів (англ. *Mandatory Access Control, MAC*) [70-80].

З ростом мереж з'явилась необхідність в обмеженні доступу до критичних об'єктів. Так з'явився механізм контролю доступу на основі ідентифікації (англ. *Identity-Based Access Control, IBAC*), який використовує списки контролю доступу (англ. *Access Control List*). Кожен суб'єкт має свій список. Тільки надавши доказ свого повноваження, користувач отримує доступ до об'єкту. Він може мати різні привілеї (на читання, запис, редагування, видалення та інші). Власник об'єкта визначає доступні операції для кожного суб'єкта. Таким чином, через необхідність

ручного контролю і можливі помилки при анулюванні права доступу суб'єкти можуть несанкціоновано отримувати більше привілеїв, ніж визначено в політиці [70-80].

Рішенням багатьох проблем, пов'язаних з попередніми видами контролю доступу, є модель на основі ролей (англ. *Role-Based Access Control, RBAC*). В ній всі ролі мають свої набори привілеїв. Кожному суб'єкту комп'ютерної системи (наприклад, СУБД або операційній системі) виділяється одна роль, на відміну від можливих реальних організацій, де користувач може мати їх декілька. В момент запиту механізм контролю доступу визначає роль, і приписаний до неї набір операцій дозволяється виконувати. Роль може розглядатися як атрибут суб'єкта. З поширенням моделі RBAC збільшилася централізованість управління доступом і відпала необхідність в списках ACL.

ACL і RBAC є окремими випадками механізму ABAC, головною ідеєю якого є визначення контролю за атрибутами сутностей, залучених в систему. Для реалізації ACL в рамках ABAC атрибутом є ідентичність, для RBAC – роль. Головною відмінністю цих двох моделей ABAC є поняття політик, виражених через певний набір логічних правил, що враховують найрізноманітніші властивості об'єкта, суб'єкта і середовища. За допомогою організації системи правил зменшуються трудовитрати на реалізацію потрібних обмежень в доступі. Крім того, при модифікації вже існуючих політик в списках контролю доступу та рольової моделі складніше врахувати всі місця, які потребують змін [81-85].

Одним з основних стандартів для управління доступом на основі атрибутів є XACML (англ. *EXtensible Access Control Markup Language*) [82-90], розроблений спочатку в 2001р. глобальним консорціумом OASIS. Цей стандарт займається регулюванням загальних концепцій безпеки в системі, а не менеджментом атрибутів, що включає призначення, модифікацію, видалення і т.д.

Головними поняттями в XACML є правила (англ. *rules*), політики (англ. *policies*), алгоритми комбінації правил і політик (англ. *rule-combining-algorithms*), атрибути (англ. *attributes*) (суб'єкта, об'єкта, дій і умов середовища), зобов'язання (англ. *obligations*) і рекомендації (англ. *advices*) [82-90]. Центральним елементом є

правило, що містить в собі за мету, ефект, умови, зобов'язання і рекомендації (двох останніх може не бути). Мета – це те, як суб'єкт бажає взаємодіяти з об'єктом (читати, редагувати, видаляти і т.д.). Ефект, який на основі обчислень логічного виразу визначається системою контролю доступу, може бути або дозволом (англ. *permit*), або відмовою (англ. *deny*), або «не застосовується» (англ. *not applicable*), або «не визначене» (англ. *indeterminate*). Рішення системи «не застосовується» приймається в разі, коли логічна умова виявляється «хибністю». При виникненні помилки під час обчислення виразу система видає «не визначене».

Більш загальним елементом структури контролю доступу є політика. Вона об'єднує кілька правил в єдину систему, пов'язану певними алгоритмами. Цієї системи і дотримується компанія. Найбільш глобальний компонент моделі – це набір політик. Існування цих компонентів зберігає модульність інфраструктури навіть на верхніх рівнях. Сукупність політик безпеки також пов'язується на основі декількох алгоритмів.

Політики можуть виражатися природною мовою (англ. *Natural Language Policy, NLP*), яка потім переводиться в зрозумілу машині мову. У великих системах від однієї організації до іншої такий опис моделі вимагає підтримки сумісності існуючих атрибутів. NLP потім транслюється в цифрові політики (англ. *digital policies, DP*), які збираються в машинний код на виконання. Для оптимізації процесу зборки може бути кілька цифрових політик, відповідних різним модулям інфраструктури. Крім цих двох видів представлення політик, існують і так звані метаполітики (англ. *metapolicy, MP*), відповідальні за регулювання, обробку ієрархій, вирішення конфліктів і перевірку коректності при компіляції цифрових політик [91-95].

Сама структура управління бізнес-моделлю ABAC складається з 4 базових механізмів, які є ключовими вузлами в реалізації політик [80-90]:

1. Механізм прийняття рішення політики (англ. *Policy Decision Point, PDP*) оцінює DP і MP і приймає рішення про доступ до об'єкта, а також є посередником між DP і MP.

2. Механізм виконання політики (англ. *Policy Enforcement Point, PEP*) реалізує рішення PDP у відповідь на запит суб'єкта про доступ до об'єкта, що захищений встановленої політикою.

3. Інформаційний пункт політики (англ. *Policy Information Point, PIP*) забезпечує PDP потрібними даними про атрибути для подальшої оцінки.

4. Механізм адміністрування політики (англ. *Policy Administration Point, PAP*) допомагає при створенні, підтримці, тестуванні і налагодженні цифрових і метаполітик, і крім того, містить відомості про політику, що проводиться.

Додатковою частиною менеджменту політики може бути застосунок для оброблення контексту (англ. *Context Handler*), який регулює процеси виконання політики безпеки та пошуку атрибутів [80-90].

Керування доступом на основі ролей (англ. *Role Based Access Control*, **RBAC**) — розвиток політики вибіркового керування доступом, при якому права доступу суб'єктів системи на об'єкти групуються з урахуванням специфіки їх застосування, утворюючи ролі [80-90].

Формування ролей покликане визначити чіткі і зрозумілі для користувачів комп'ютерної системи правила розмежування доступу. Рольове розмежування доступу дозволяє реалізувати гнучкі та динамічні змінни в процесі функціонування комп'ютерної системи правила розмежування доступу.

Таке розмежування доступу є складовою багатьох сучасних комп'ютерних систем. Як правило, даний підхід застосовується в системах захисту СУБД, а окремі елементи реалізуються в мережевих операційних системах. Рольовий підхід часто використовується в системах, для користувачів яких чітко визначено коло їх посадових повноважень і обов'язків.

Незважаючи на те, що Роль є сукупністю прав доступу на об'єкти комп'ютерної системи, рольове керування доступом аж ніяк не є окремим випадком вибіркового управління доступом, так як його правила визначають порядок надання доступу суб'єктам комп'ютерної системи в залежності від наявних (або відсутніх) у нього ролей в кожен момент часу, що є характерним для систем мандатного керування доступом. З іншого боку, правила рольового

розмежування доступу є більш гнучкими, ніж при мандатному підході до розмежування.

Так як привілеї не призначаються користувачам безпосередньо і отримуються ними тільки через свою роль (або ролі), управління індивідуальними правами користувача по суті зводиться до призначення йому ролей. Це спрощує такі операції, як додавання користувача або зміна підрозділу користувачем.

Базова модель RBAC

Для визначення моделі RBAC визначаються наступні умови:

— S = Суб'єкт = Людина або автоматизований агент (множина користувачів);

— R = Роль = Робоча функція або назва, яка визначається на рівні авторизації (множина ролей);

— P = Дозволи = Затвердження режиму доступу до ресурсу (множина прав доступу на об'єкти системи);

— SE = Сесія = Відповідність між S, R та / або P;

— SA = Призначення суб'єкта;

— PA: R→2p — функція, що визначає для кожної ролі множину прав доступу; при цьому для кожного p ∈ P існує r ∈ R така, що p ∈ PA (r);

— RH = Частково впорядкована ієрархія ролей. RH може бути ще записана так:

- Один суб'єкт може мати кілька ролей.
- Одну роль можуть мати декілька суб'єктів.
- Одна роль може мати кілька дозволів.
- Один дозвіл може належати кільком ролям.

Ролі призначаються суб'єктам, внаслідок чого суб'єкти отримують ті чи інші дозволи через ролі. RBAC вимагає саме такого призначення, а не прямого призначення дозволів суб'єктам, інакше це призводить до складно контрольованих відносин між суб'єктами і дозволами [85-95].

На можливість успадкування дозволів від протилежних ролей накладається обмежувальна норма, яка дозволяє досягти належного поділу режимів.

Наприклад, одній і тій же особі може бути не дозволено створити обліковий запис для когось, а потім авторизуватися під цим обліковим записом.

Використовуючи нотацію теорії множин:

— $PA \subseteq P \times R$, при цьому дозволи призначаються зв'язкам ролей у відношенні «багато до багатьох».

— $SA \subseteq S \times R$, при цьому суб'єкти призначаються зв'язкам ролей і суб'єктів у відношенні «багато до багатьох».

— $RH \subseteq R \times R$.

Позначення: x ≥ y означає, що x успадковує дозволи y.

Суб'єкт може мати множину одночасних сесій з різними дозволами.

Технологія керування доступом на основі ролей досить гнучка і сильна, щоб змоделювати як вибіркове керування доступом (DAC) [85-90], так і мандатне керування доступом (MAC) [90-95].

До розробки RBAC, єдиними відомими моделями управління доступом були MAC і DAC: якщо модель була MAC, то вона була DAC, і навпаки. Дослідження в 90-х показали, що RBAC не потрапляє ні в ту, ні в іншу категорію.

Ролі створюються всередині організації для різних робочих функцій. Певним ролям присвоюються повноваження (permissions) для виконання тих чи інших операцій. Штатним співробітникам (або іншим користувачам системи) призначаються фіксовані ролі, через які вони отримують відповідні привілеї для виконання фіксованих системних функцій. На відміну від управління доступом на основі контексту (англ. *Context-based access control*, CBAC), реалізація RBAC в чистому вигляді не враховує поточну ситуацію (таку як, наприклад, звідки було встановлено з'єднання).

RBAC відрізняється від списків контролю доступу (англ. *Access control lists*, ACL), які використовуються в традиційних вибіркових системах управління доступом, тим, що може давати привілеї на складні операції зі складовими даними, а не тільки на атомарні операції з низькорівневими об'єктами даних.

Концепції ієрархії ролей і обмежень дозволяють створити або змоделювати контроль доступу на основі решітки (англ. *Lattice-based access control*, LBAC) засобами RBAC. Таким чином, RBAC може бути основою і розширенням LBAC.

Привабливою можливістю є використання самої RBAC для сприяння децентралізованому управлінню RBAC.

RBAC широко використовується для управління призначеними для користувача привілеями в межах єдиної системи або єдиного додатку. Список таких систем включає в себе Microsoft Active Directory, SELinux, FreeBSD, Solaris, СУБД Oracle, PostgreSQL 8.1, SAP R / 3, Lotus Notes і безліч інших.

Таблиця 1.2.1

Аналіз основних методів розмежування доступу

Метод	D	S	E	R	P	K	H
Бела-ЛаПадули	+	-	-	Z	-	-	-
Довірених суб'єктів	+	-	+	X	-	-	-
Розподілених систем	+	-	+	C	-	-	-
Адепт-50	+	-	-	C	-	-	-
LWM	+	-	+	Z	-	-	-
Лендвера	+	-	+	V	-	-	-
MAC	+	+	+	X	-	-	-
HRU	+	+	-	B	-	-	-
Кларка-Вілсона	+	-	-	Z	-	-	-
Міллена (MPP)	+	-	+	Z	-	-	-
MMS	R+	+	+	M	-	-	-
Біба	R-	-	-	N	-	-	-
На основі ролей	+	-	-	C	-	-	-
На основі атрибутів	+	-	-	C	-	-	-

Узагальнимо аналіз основних методів розмежування доступу (див. табл.1.2.1), введемо для цього позначення: D – типи доступу, що використовуються в моделі; S – системний компонент; E – компонент безпеки; R – особливості операцій доступу суб'єкта до об'єктів; «R+» – Read, write, create, delete операції над об'єктами специфічної структури; «R–» – обмеження R/W; Z – обмеження накладаються на найпростіші операції r/w; X – операції read, write можуть бути видаленими; C – забезпечує однорідний контроль права на доступ над неоднорідною безліччю 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 впорядковані відповідно до рівнів безпеки; M – крім найпростіших операцій в моделі можуть з'явитися операції, спрямовані на специфічну обробку інформації; P – можливість

підключення паралельного механізму розмежування доступу; К – наявність мультипотокового механізму захисту; Н – наявність ієрархії рівнів доступу [75-90].

Підсумовуючі можно зауважіті что класічні моделі розмежування доступу не розраховані на розподілене зберегання даних. Більш сучасні теж не враховуют паралельній характер обробки данних та потребують адаптації для задовільненя цих потреб.

1.3. Аналіз системно-концептуального підходу до побудови систем захисту інформації

На загальному рівні систему захисту інформації визначено [35, 72] як організаційну сукупність всіх засобів, методів та заходів, що виділяються (надаються) АСОД для задоволення обраних завдань захисту. Це поняття постулює той факт, що всі ресурси, виділені для захисту інформації, повинні бути об’єднані в єдину цілісну систему, яка є функціонально незалежною підсистемою АСОД. Ієрархію вимог до системі захисту інформації зручно відобразити графічно (див. рис. 1.3.1).

Рисунок 1.3.1 – Сукупність вимог до системи захисту інформації в АСОД

Дотримання цих вимог, як правило, сприяє покращенню захисту. В умовах системно-концептуального підходу до захисту необхідно не просто керуватися певними загальними положеннями - потрібна цілісна і, можливо, більш повна система загальних методологічних принципів [35, 72]. Сформована система включає загальнометодологічні принципи: концептуальна єдність; адекватність; гнучкість; функціональна самостійність; зручність використання; мінімізація прав; повний контроль; адекватне реагування; економічність.

Архітектура СЗІ, на базі цих принціпів, повинна бути схожа на архітектуру АСОД і мати функціональну, організовану і структурну побудову.

Відповідно до приведеної схеми (див. рис. 1.3.2), організаційно СЗІ складається з трьох частин: механізмів захисту інформації, механізмів управління механізмами захисту та механізмами загальної організації системи. З точки зору проводимого дослідження найбільший інтерес викликає виділення механізмів управління механізмами захисту. Але наведенная авторами системно-концептуального підходу до захисту класифікація АСОД, суттєво обмежує використання цієї переваги. Множина типів АСОД включає персональна електронна обчислювальна машина, що використовується локально; групова електронна обчислювальна машина, що використовується локально; обчислювальний центр підприємства, установи, організації; обчислювальний центр колективного користування; локальна обчислювальна мережа; слаборозподілені (в межах населеного пункту, невеликої території) обчислювальні мережі; сильнорозподілені, регіональні обчислювальні мережі; глобальні обчислювальні мережі. Відповідно застаріла класифікація потребує переосмислення запропонованих підходів в сучасних умовах.

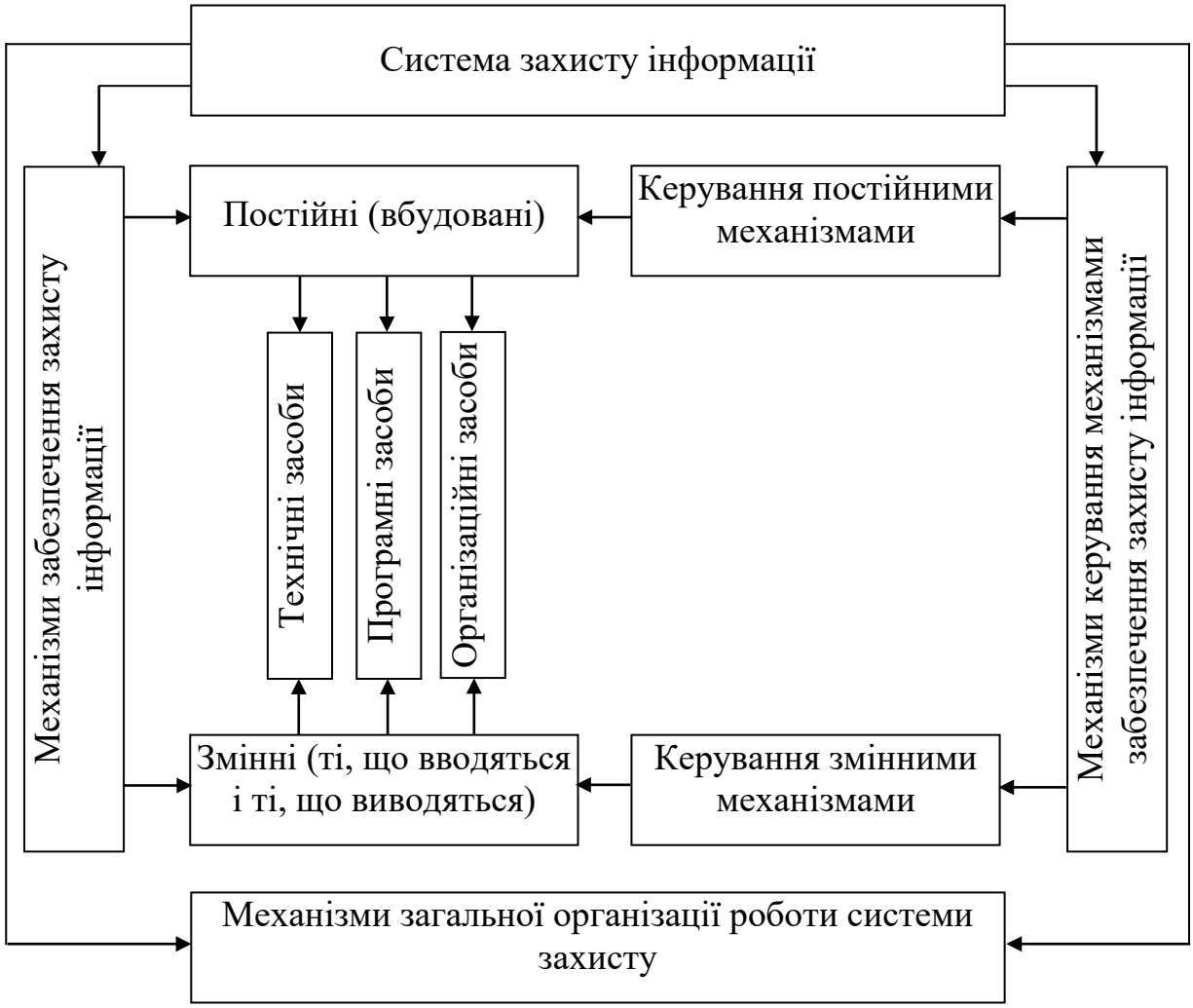


Рисунок 1.3.2 – Організаційна побудова системи захисту інформації

Послідовність і зміст проектування систем захисту інформації, які наведені на рисунку 1.3.3, потребують більш сучасної інтерпретації в пунктах 3 и 4.

На наступних рисунках використовується скорочення: КНОІ – канал несанкціонованого отримання інформації.

Рисунок 1.3.3 – Послідовність і зміст проектування систем захисту інформації

Формалізовані постановки задач проектування наведені в [1]. Класифікаційна структура задач, які підлягають вибору в процесі проектування СЗІ (див. рис. 1.3.4) зберегла свою актуальність.

На даному рисунку, крім вищезазначеного, використовується скорочення: ДФ – дестабілізуючі фактори.

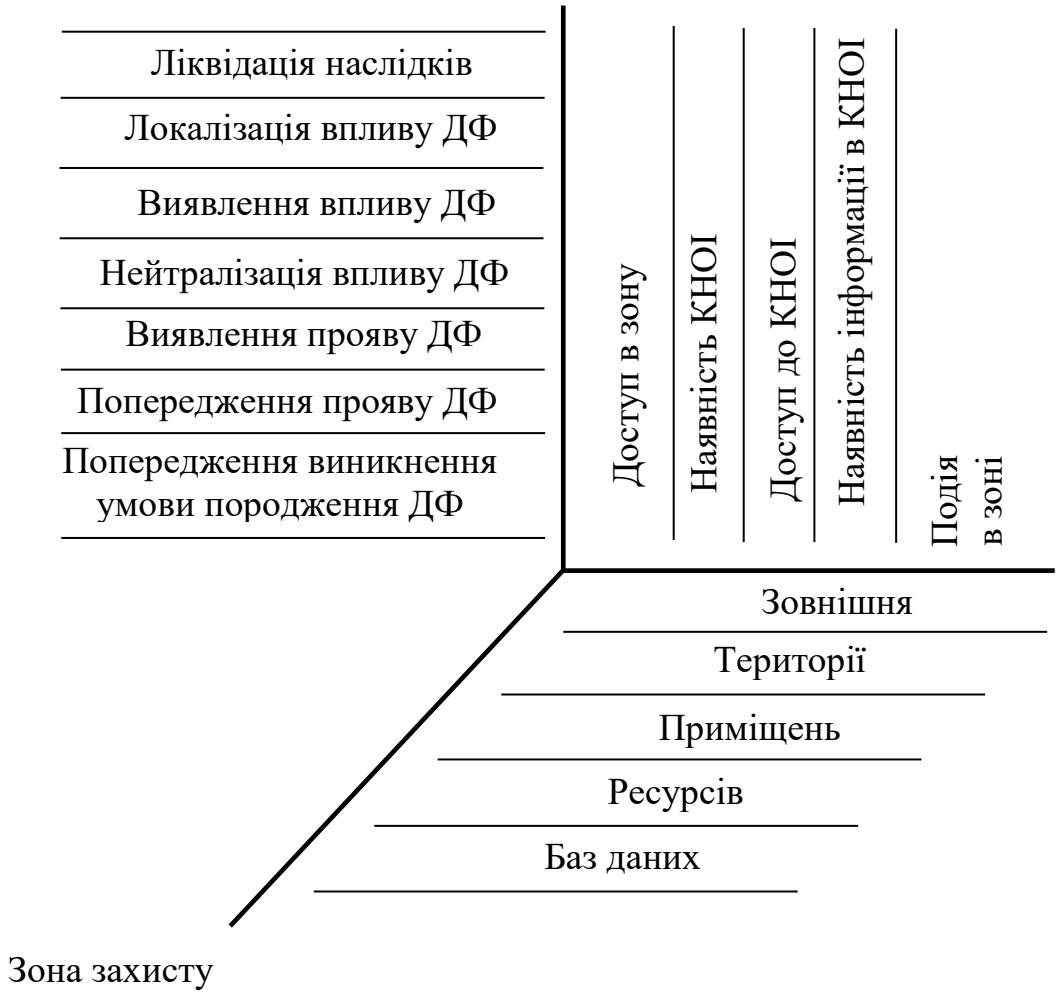


Рисунок 1.3.4 – Класифікаційна структура задач, що підлягають вибору в процесі проектування СЗІ

Загальна модель керування захистом інформації (див. рис. 1.3.5) застосується на етапе функціонування СЗІ і має бути адаптована до реального алгоритму обробки інформації.

На даному рисунку використовуються наступні скорочення: з.вим. – захист, що вимагається; з.оч. – захищеність інформації, що очікується; P – рівень; $P_{д.з.}$ – дійсний рівень захищеності; доп. – допустиме значення.

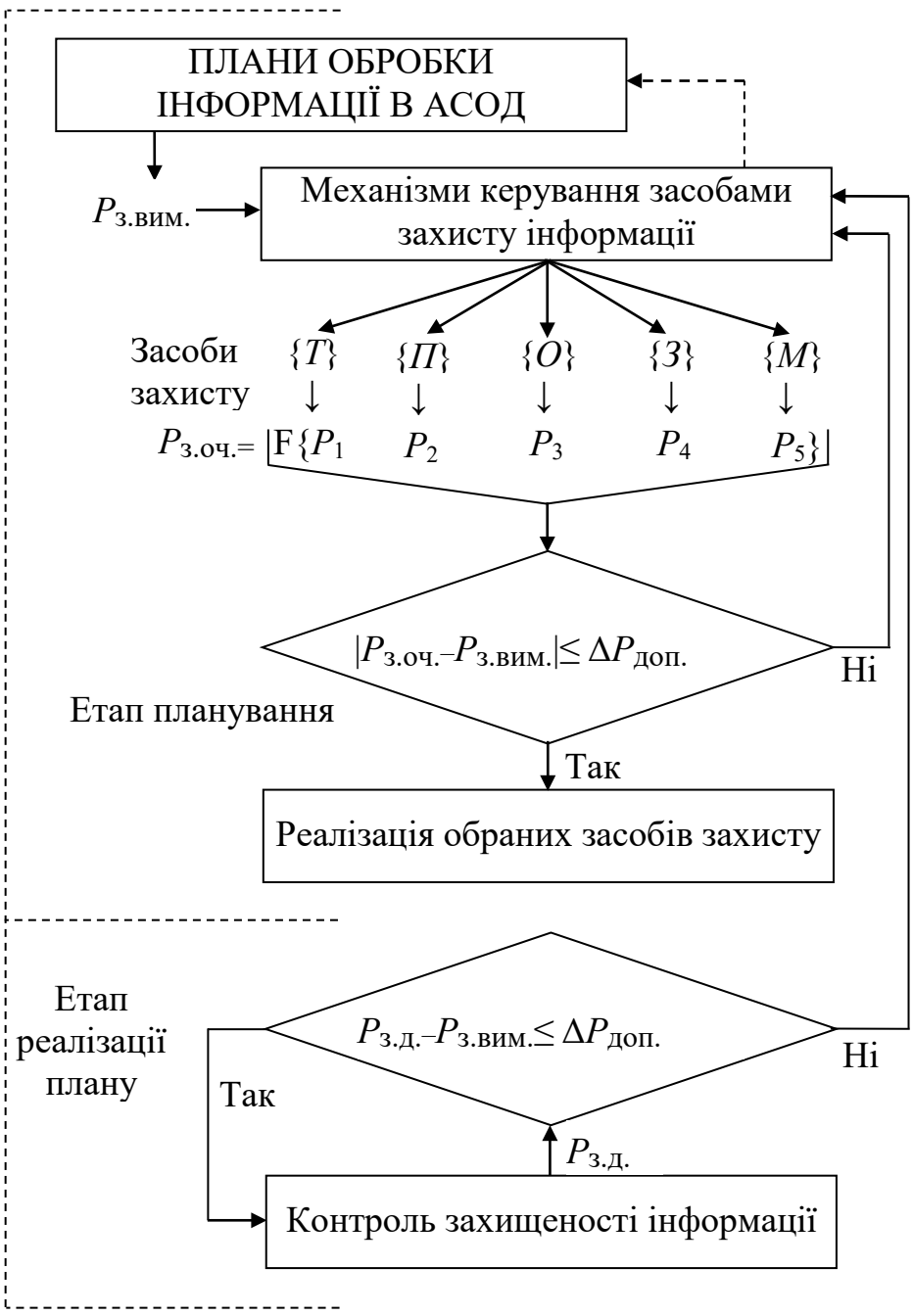


Рисунок 1.3.5 – Загальна модель керування захистом інформації

В цілому системно-концептуального підхід до захисту інформації зберіг свою актуальність та має бути застосованій до побудові нових методів та моделей, як комплексних систем захисту інформації так і окремих механізмів захисту. Більш сучасним є функціонально-орієнтований підхід повязаній з застосуванням мобільних мереж Next Generation Networks розглянемо його більш детально.

1.4. Аналіз розвитку мереж розподіленої обробки та зберегання інформації

Популярним трендом розвитку телекомунікаційних та комп'ютерних мереж є бездротові технології, які використовують повітря як середовище розповсюдження. Зручність цього підходу в мобільності користувачів та незалежності контенту від розташування точок доступу. Поява мобільних пристроїв, таких як смартфони, планшеті або нетбуки, завдяки їх оснащенню кількома інтерфейсами, дозволяє мобільним користувачам отримувати доступ до мережевих послуг та обміну інформацією будь-де і в будь-який час. Для підтримки стану завжди на зв'язку (always-connected), телекомунікаційні мережі еволюціонують в напряму розвитку інтернет протоколів таким чином, що ядро IP мережі буде діяти як точка підключення для наявного набору мереж на основі різних бездротових технологій. Цей майбутній сценарій, який називається мережами наступного покоління [94] Next Generation Networks (NGNs), дозволяє здійснювати конвергенцію різних гетерогенних бездротових мереж доступу, які об'єднують всі переваги, що пропонуються кожним бездротовим доступом до мережі. Розглянемо деякі з моделей контролю доступу що застосовуються при цьому.

В першу чергу нагадаєм [94] загальну постановку задачі. Мережі наступного покоління призначені бути мобільними. Користувач, озброєний мульти-інтерфейсними легкими пристроями, побудованими на бездротових технологіях, отримує свободу виконання рухів та змін місць розташування зберігаючи доступ до мережевих послуг, таких як VoIP або потокове відео. Поняття мобільності вимагає безперервності сесії, коли користувач рухається по різних частках мережі. Іншими словами, активні комунікації повинні підтримуватися без збоїв, коли користувач змінює свою точку підключення до мережі під час руху. Саме це є принциповою перевагою NGNs користувачеві мають рухатись між різними сегментами мережами, не відчуваючи тимчасового переривання або значної затримки в активних комунікаціях. Відповідна процедура має назву handoff

process або автоматичне перепідключення. Реалізація цього процесу потребує вирішення низки задач [96], що негативно впливає на латентність перепідключення. Зокрема, перевірки в процесі автентифікації та розподіл ключів є найбільш кричними оскільки вони вимагають значного часу [97-100]. Їх реалізація під час процесу контроля доступу має забезпечити санкціонованість доступу, надійну реєстрацію та облік. Цього вимагає комерційній характер надання послуг зв'язку.

Розглянемо підходи, які були запропоновані для вирішення цієї складної проблеми у мережах наступного покоління NGN. Точніше, ми збираємося виконувати цей аналіз у контексті розширюваного протоколу автентичності (EAP), протоколу, який має важливе значення для реалізації рішень контролю доступу у NGN.

Підтримка санкціонованого доступу до мережевої служби у NGN гарантується шляхом розгортання так званої інфраструктури автентифікації, авторизації та обліку *Authentication, Authorization and Accounting* (AAO) [94, 101]. AAO визначає фреймворк для координації дії власних служб безпеки на крос платформах та технологіях поєднаних у мережі.

AAO надає наступні послуги:

— автентифікація. Ця послуга забезпечує дію механізму ідентифікації користувача, який вимагає доступу до деякої служби (наприклад, доступу до мережі). Під час процесу автентифікації користувачі надають набір повноважень (наприклад, пароль або сертифікат), щоб підтвердити, що вони є, якими вони стверджують. Тільки тоді, коли облікові дані правильно підтверджуються сервером AAO, користувач отримує доступ до послуги.

— авторизація. Авторизація, як правило, базується на автентифікації та являє собою процес визначення того, чи дозволяється клієнт виконувати та вимагати певних завдань або операцій. Авторизація - це процес виконання політики, яка визначає права щодо типів діяльності, ресурсів або послуг санкціонованих для користувача.

— облік. Третій компонент у рамках AAO - облік, який вимірює ресурси,

користувач споживає під час доступу до мережі. Прикладом цього є кількість часу використання службі або кількість даних користувач надіслав та / або отримав під час сеансу.

Загальна архітектура ААО , яку визначено [101], вимагає участі чотирьох різних суб'єктів (див. рис. 1.4.1), що беруть участь у процесах автентифікації, авторизації та бухгалтерського обліку:

— Користувач, який бажає отримати доступ до специфічної служби, запропонованої оператором мережі.

— Домен, де користувач зареєстрований. Цей домен, як правило, називається домашній домен, здатний перевірити ідентифікацію користувача на основі деяких облікових даних. Домашній домен може не тільки автентифікувати, але також забезпечує інформації для авторизації користувачеві.

— Постачальник послуг, що контролює доступ до запропонованих послуг. Постачальник послуг може бути зареєстрований у домені, де користувач підписаний (домашній домен) або у іншому доменом у випадках роумінгу.

— Сервісне обслуговування послуг (сервіс), яке буде, як правило, розташоване на пристрої, що належить до постачальника послуг. Наприклад, у випадку служби доступу до мережі, цю роль відтворює сервер доступу до мережі (NAS), наприклад, у вигляді точки доступу 802.11.

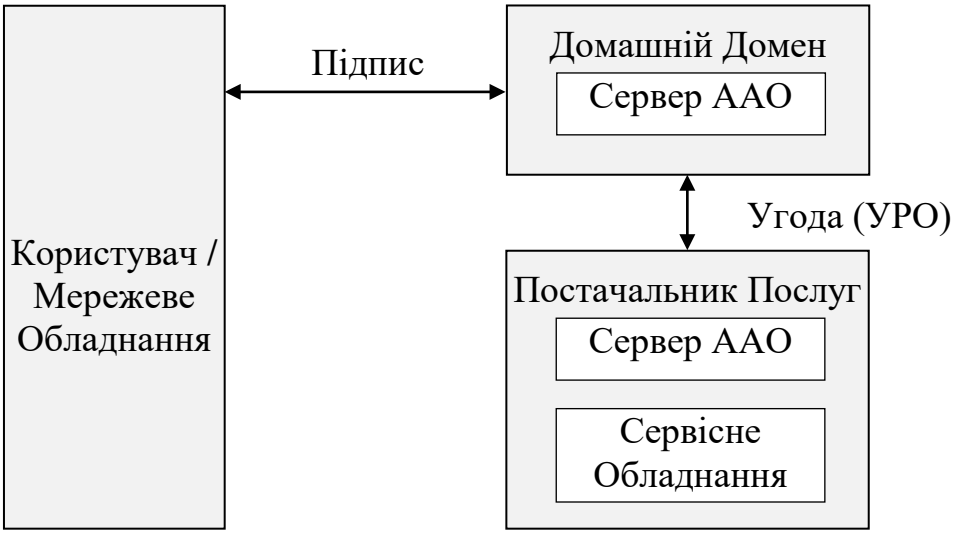
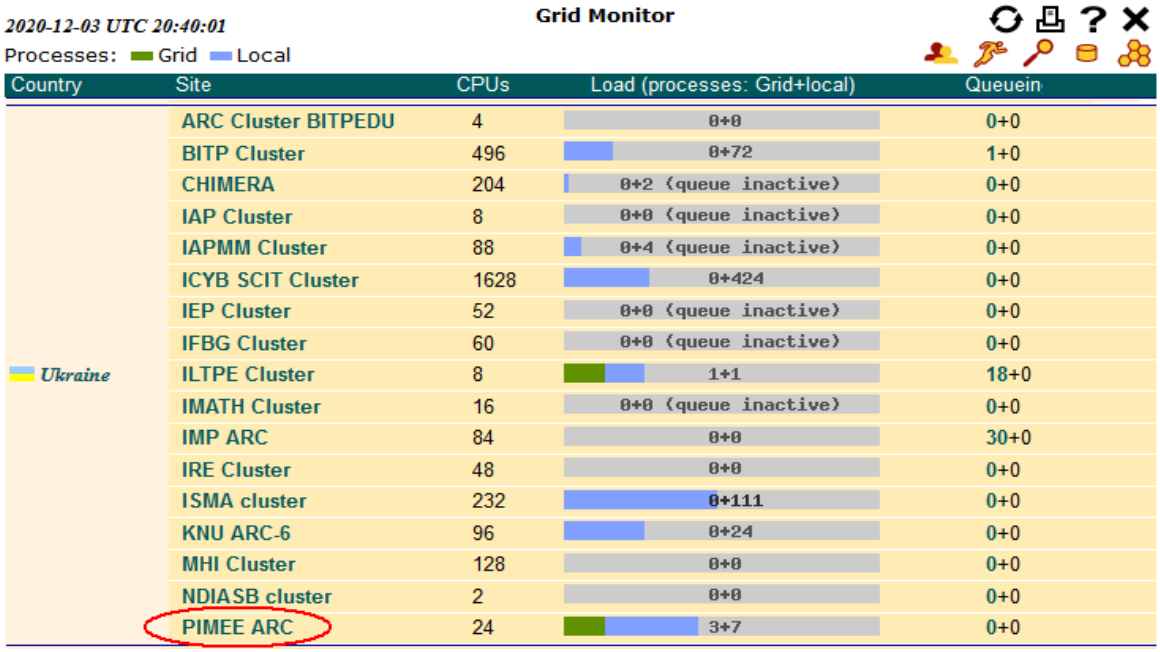


Рисунок 1.4.1 – Загальна архітектура ААО

Системи доступу до інформаційних ресурсів, які розміщені у комп'ютерних мережах є одним з головних компонент структури локальних мереж або інших фрагментів глобальної мережі. Системи доступу реалізують певні функції захисту інформаційних ресурсів, за якими звертаються окремі користувачі. Оскільки окремі локальні мережі або фрагменти глобальної мережі є функціонально орієнтованими, то способи організації відповідних систем доступу, можливості контролю прав доступу, які вони реалізують, є теж функціонально орієнтованими. Це приводить до того, що такі системи є розподіленими не тільки на рівні розмірів фрагментів мережі але й на рівні особливостей задач доступу, які вони вирішують. Наприклад, у випадку організації доступу до баз даних вирішуються задачі перевірки повноважень, задачі модифікації повноважень і ряд інших задач пов'язаних із забезпеченням доступу, орієнтованого винятково на читання, запис або, припустимих у рамках структури бази даних, перетворень відповідних даних. При цьому, ідентифікація в системах керування базами даних вирішується на рівні використання паролів, які привласнюються користувачам. Відомі моделі захисту даних, в основному, пов'язані з аналізом параметрів, які характеризують самі дані з погляду їхньої доступності окремим користувачам і, у першу чергу, аналізують взаємини між параметрами, які характеризують міру їхньої доступності. Другим прикладом специфіки роботи системи доступу можуть служити системи, у яких основні функції захисту покладено на процеси й моделі ідентифікації користувачів, які претендують на використання ресурсів. Засоби, які застосовуються для цих цілей, мають досить розвинений апарат криптографії, що ґрунтується на криптографічних алгоритмах, протоколах автентифікації й цілому ряді інших досить потужних засобів реалізації розмежування доступу.

Базові данні для аналізу спеціалізованих розподілених інформаційних систем було отримано на кластері Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. Далі наведені дані (див. рис. 1.4.2) щодо використання грід-ресурсів під час проведення експериментів.



2020-12-03 UTC 20:40:01

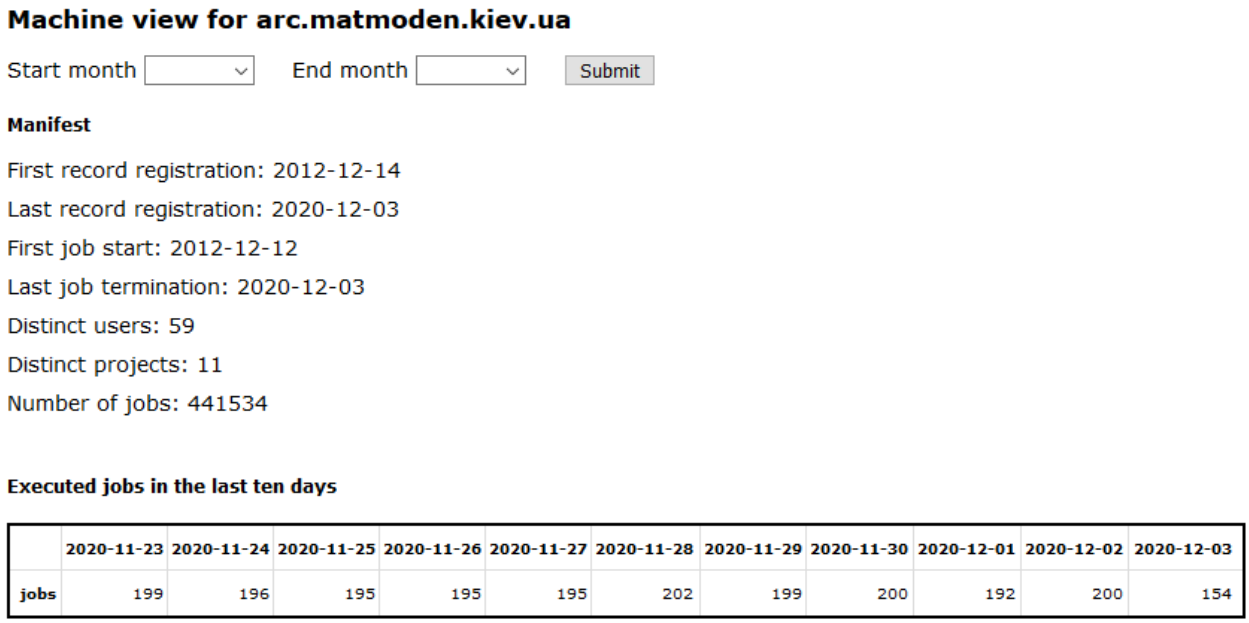
Grid Monitor

Processes: Grid Local

Country	Site	CPUs	Load (processes: Grid+local)	Queuein
	ARC Cluster BITPEDU	4	0+0	0+0
	BITP Cluster	496	0+72	1+0
	CHIMERA	204	0+2 (queue inactive)	0+0
	IAP Cluster	8	0+0 (queue inactive)	0+0
	IAPMM Cluster	88	0+4 (queue inactive)	0+0
	ICYB SCIT Cluster	1628	0+424	0+0
	IEP Cluster	52	0+0 (queue inactive)	0+0
	IFBG Cluster	60	0+0 (queue inactive)	0+0
Ukraine	ILTPE Cluster	8	1+1	18+0
	IMATH Cluster	16	0+0 (queue inactive)	0+0
	IMP ARC	84	0+0	30+0
	IRE Cluster	48	0+0	0+0
	ISMA cluster	232	0+111	0+0
	KNU ARC-6	96	0+24	0+0
	MHI Cluster	128	0+0	0+0
	NDIASB cluster	2	0+0	0+0
	PIMEE ARC	24	3+7	0+0

Рисунок 1.4.2 – Моніторинг використаних ресурсів грід-сайту ІПМЕ ім. Г.Є. Пухова НАН України 03.12.2020 р. згідно даним сайту http://www.nordugrid.org/monitor

Дані підтверджують гібридний характер навантаження (3 грід задачі, 7 локальних) що показує їх репрезентабільність. Наступні дані (див. рис.1.4.3)



Machine view for arc.matmoden.kiev.ua

Start month End month Submit

Manifest

First record registration: 2012-12-14

Last record registration: 2020-12-03

First job start: 2012-12-12

Last job termination: 2020-12-03

Distinct users: 59

Distinct projects: 11

Number of jobs: 441534

Executed jobs in the last ten days

	2020-11-23	2020-11-24	2020-11-25	2020-11-26	2020-11-27	2020-11-28	2020-11-29	2020-11-30	2020-12-01	2020-12-02	2020-12-03
jobs	199	196	195	195	195	202	199	200	192	200	154

Рисунок 1.4.3 – Використання ресурсів грід-сайту ІПМЕ ім. Г.Є. Пухова НАН України наприкінці листопада 2020 р. згідно даним системи SGAS (https://vobox1.bitp.kiev.ua:6143/sgas/view/machines/arc.matmoden.kiev.ua)

ілюструють середню завантаженість в 200 задач доба віртуальної організації matmoden протягом декади (стандартній період моніторингу) згідно даним системи SGAS.

Також підтверджена (див. рис.1.4.4) стабільність параметрів протягом року (2020 рік евромоніторинг система ARGO частка EGI).

Таким чином базовими параметрами є стабільне та коректне функціонування дослідного зразка спеціалізованої розподіленої інформаційної системі грід-сайту PIMEE ARC в складі Українського національного гріду, виконуючі як локальні задачі, так и грід-завдання. При щодобовому навантаженні близько 200 грід-завдань (з яких приблизно половина – службові задачі). Коефіцієнти готовності та надійності грід-вузлу UA-PIMEE за минулий час поточного року приймали середньомісячні значення у діапазоні 86,76% – 100%. Ці данні є базовими при проведенні експериментів, якщо це не оговорюється окремо.

UA-PIMEE DETAILS

Timestamp	Availability	Reliability	Unknown	Downtime
2020-01	99.76	99.76	0	0
2020-02	100	100	0	0
2020-03	86.76	99.92	0	13
2020-04	98.82	98.82	0	0
2020-05	96.43	96.43	0	0
2020-06	100	100	0	0
2020-07	98.52	98.52	0	0
2020-08	98.45	98.45	0	0
2020-09	99.53	99.53	0	0
2020-10	99.38	99.38	0	0
2020-11	99.14	99.14	0	0
2020-12	100	100	0	0

Рисунок 1.4.4 – Доступність та надійність грід-сайту ІПМЕ ім. Г.Є. Пухова НАН України за 2020 р. згідно даним системи ARGO (https://argo.egi.eu/egi/report-ar-dates-2/Critical/SITES/UA-PIMEE?start_date=2020-01-01&end_date=2020-12-01)

Система, яка орієнтована на захист засобів доступу повинна являти собою досить універсальний засіб, у рамках якого існує можливість здійснювати такі зміни в системі доступу, які приводили б до зміни рівня їхніх можливостей по захисту інформаційних ресурсів, які такі системи обробляють. Відповідні зміни розглянуті як реалізація процесів керування системою доступу. Функціональна блок схема загальної структури організації засобів захисту й системи її адаптації наведена на рисунку 1.4.5.

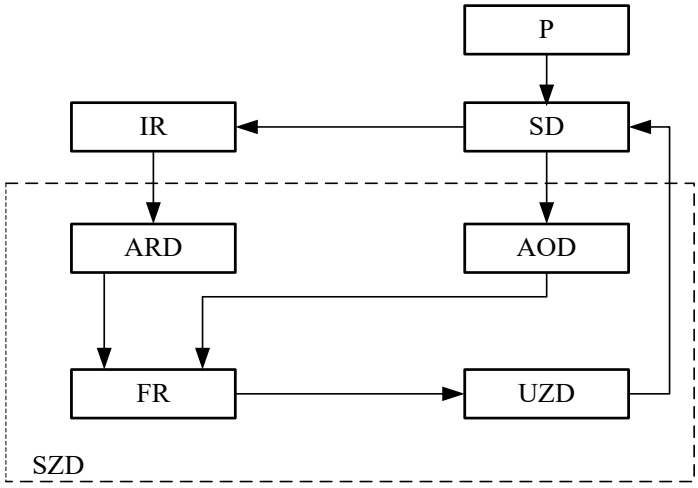


Рисунок 1.4.5 – Загальна функціональна схема системи захисту доступу до інформаційних ресурсів

На рисунку використовуються наступні позначення: *P* - користувач; *IR* - інформаційні ресурси; *SD* - система керування доступом; *ARD* - аналіз результатів реалізованого доступу; *AOD* - аналіз ситуації у випадку, коли в доступі користувачеві відмовлено; *FR* - формування рішень для засобів захисту за поточним станом системи доступу; *UZD* - керування засобами захисту системи доступу до інформаційних ресурсів; *SZD* - система захисту доступу.

Далі у роботі буде показано, що для реалізації модулів *ARD* і *AOD* доцільно використовувати нейроні мережі, які на етапі інсталяції можуть бути навчені відомим ситуаціям в *IR* і *SD*, які створюються у відповідних модулях і які відповідають різним рівням безпеки системи керування доступом. Використання

нейронних мереж для реалізації *ARD* та *AOD* у рамках *SZD* обумовлено ще й тим, що в процесі функціонування системи доступу з боку потенційних користувачів можуть ініціюватися такі способи взаємодії системи доступу з користувачем, які відповідають новим типам небезпечних ситуацій, зразки яких на момент інсталяції відповідних модулів могли не існувати. Нейроні мережі в процесі функціонування можуть розвиватися і в процесі такого розвитку формувати нові зразки.

1.5. Висновки до першого розділу

У першому розділі проведено аналіз поточного стану методів та моделей розмежування доступу до ресурсів інформаційних систем. Для цього виконано аналіз топології інформаційної безпеки Українського національного гріду, аналіз моделей розмежування доступу до ресурсів інформаційних систем, аналіз системно-концептуального підходу до побудові систем захисту інформації та аналіз розвитку мереж розподіленої обробки та зберегання інформації.

Встановлено, що однопотокові механізми розмежування доступу не можуть забезпечити високі вимоги для високопродуктивної обробки інформаційних ресурсів з обмеженим доступом, в той же час спостерігається постійне зростання продуктивності обчислювальних систем, тому запропоновано наділити підсистему захисту властивостями адаптації по відношенню до критеріїв, які визначаються параметрами стану безпеки системи та параметрами, що характеризують процеси обробки інформації у спеціалізованих розподілених інформаційних системах.

Список використаних джерел до першого розділу

1. Украинский академический грид / А.Г. Загородний, Г.Е. Зиновьев, Е.С. Мартынов, С.Я. Свистунов – Українсько-македонський науковий збірник.: Випуск 4, Київ – 2009, Вид. Національна бібліотека України імені В.І.Вернадського, С.140-150.

2. Практикум з грід-технологій: навчальний посібник / А.І. Петренко, С.Я. Свістунов, Г.Д. Кисельов – К.: НТУУ «КПІ», 2011. – 580 с.

3. ПОЛОЖЕННЯ про Український Національний Грід (УНГ) [Електронний ресурс]. – Режим доступа: http://infrastructure.kiev.ua/upload/ung_fin.pdf.

4. ПРАВИЛА використання ресурсів Українського Національного Гріда (УНГ) [Электронный ресурс]. – Режим доступа: http://infrastructure.kiev.ua/upload/ resources_fin.pdf.

5. ПОЛОЖЕННЯ про Базовий координаційний грід-центр Українського Національного Гріду [Електронний ресурс]. – Режим доступа: http://infrastructure.kiev.ua/ upload/bcc_fin.pdf.

6. ПРАВИЛА І ПРОЦЕДУРА реєстрації грід-сайтів Українського Національного Гріду (УНГ) [Електронний ресурс]. – Режим доступа: http://infrastructure.kiev.ua/ upload/grid-site_fin.pdf.

7. Правила і процедура створення та реєстрації віртуальних організацій Українського Національного Гріду [Електронний ресурс]. – Режим доступа: http://infrastructure.kiev.ua/upload/grid-site_fin.pdf.

8. Advanced Resource Connector // NORDUGRID [Електронний ресурс]. – Режим доступа: http://www.nordugrid.org/arc.

9. Інсталяція ARC2 [Електронний ресурс]. – Режим доступа: http://grid.org.ua/wiki/ tech/arc1.

10. Реєстрація грід-сайтів [Електронний ресурс]. – Режим доступа: http://ung.in.ua/ ua/join.

11. Реєстрація ВО [Електронний ресурс]. – Режим доступа: http://ung.in.ua/ua/ vo_registration.

12. UA-Grid: Украинская национальная грид-программа / А.Г. Загородний, С.Я. Свистунов, Л.Ф. Белоус, А.Л. Головинский // International Conference "Parallel and Distributed Computing Systems" PDCS 2013(Ukraine, Kharkiv, March 13-14, 2013), pp.346-356

13. Operations Portal [Електронний ресурс]. – Режим доступа: http://operations-portal.egi.eu.

14. EGI Accounting Portal [Електронний ресурс]. – Режим доступа: http:// accounting.egi.eu

15. Welcome to EGI Helpdesk [Електронний ресурс]. – Режим доступа: http://helpdesk.egi.eu.

16. Welcome to GOCDB [Електронний ресурс]. – Режим доступа: https://goc.egi.eu.

17. Реєстрація ресурсного центру [Електронний ресурс]. – Режим доступа: http://grid.org.ua/wiki/roc/rc_reg.

18. PROC09 Resource Centre Registration and Certification [Электронный ресурс]. – Режим доступа: https://wiki.egi.eu/wiki/PROC09.

19. HOWTO01 Site Certification Required Information [Електронний ресурс]. – Режим доступа: https://wiki.egi.eu/wiki/HOWTO01_Site_Certification_Required_Information.

20. HOWTO02 Site Certification Required Documentation [Електронний ресурс]. – Режим доступа: https://wiki.egi.eu/wiki/HOWTO02_Site_Certification_Required_Documentation.

21. Grid Site Operations Policy [Электронный ресурс]. – Режим доступа: https://documents.egi.eu/public/ShowDocument?docid=75.

22. GGUS – the EGI Helpdesk [Електронний ресурс]. – Режим доступа: https://ggus.eu.

23. Практикум з грід-технологій: навчальний посібник / А.І. Петренко, С.Я. Свістунов, Г.Д. Кисельов – К.: НТУУ «КПІ», 2011. – 580 с.

24. ГридННС Мониторинг и Аккаунтинг // Информационный портал ОИЯИ [Електронний ресурс]. – Режим доступа: http://grid.jinr.ru/?page_id=749.

25. UGRID. Ukrainian Academical grid monitoring [Електронний ресурс]. – Режим доступа: https://194.44.37.211/nagios.

26. Nagios [Електронний ресурс]. – Режим доступа: http://www.nagios.org.

27. Advanced Resource Connector // NORDUGRID [Електронний ресурс]. – Режим доступа: http://www.nordugrid.org/arc.

28. Инфраструктура [Електронний ресурс]. – Режим доступа: http://infrastructure.kiev.ua.

29. Грид-монитор [Електронний ресурс]. – Режим доступа: http://gridmon.bitp.kiev.ua.

30. SGAS View Page [Електронний ресурс]. – Режим доступа: https://vobox1.bitp.kiev.ua:6143/sgas/view.

31. А. П. Баранов, Н. П. Борисенко, П. Д. Зегжда, А. Г. Ростовцев, Корт С. С. — Математические основы информационной безопасности. — М.: Издательство Агентства «Яхтсмен», 1997. С 22-36

32. Хоффман Дж. Современные методы защиты информации. - М.: Сов. радио, 1980.

33. Bell L. LaPadula. Secure Computer System: Mathematical Foundation, ESD-TR-73-278, V 1, MITRE Corportation.

34. LaPadula D. Bell. Secure Computer Systems: A Mathematical Model, ESD TR-73-278, V. II, MITRE Corportaion.

35. Герасименко В.А., Малюк А.А. Основы защиты информации. - Москва: МИФИ, 1997. — 537 с.

36. Зегжда Д. П. Как построить защищённую информационную систему / Д. П. Зегжда, А. М. Ивашко. — СПб. : Мир и семья, 1997. — 312 с.

37. Смит Р. Э. Аутентификация: от паролей до открытых ключей / Р. Э. Смит. — М. : Вильямс, 2002. — 432 с.

38. Хорошко В. А. Методы и средства защиты информации / В. А. Хорошко, А. А. Чекатков. — К. : Юниор, 2003. — 504 с.

39. Зима В. М. Безопасность глобальных сетевых технологий / В. М. Зима, А. А. Молдовян, Н. А. Молдовян. — СПб. : БХВ-Петербург, 2000. — 320 с.

40. Nyanchama M. Modeling mandatory access control in role-based security systems / M. Nyanchama, S. Osborn // InDBSec. — 1995. — P. 129–144.

41. 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.

42. Cotrini C. Analyzing first-order role based access control / C. Cotrini, T. Weghorn, D. Basin, M. Clavel. — 2015.

43. J.Rushby, Formal methods and their role in the certification of critical systems, 1995.

44. Модель Take-Grant. [Електронний ресурс]. – Режим доступа: https://uk.wikipedia.org/wiki/%D0%9C%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C_Take-Grant

45. Daniel Servos, Sylvia L. Osborn. Current Research and Open Problems in Attribute-Based Access Control. — University of Western Ontario.

46. Vincent C. Hu, etc. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. — National Institute of Standards and Technology, 2014. — P. 45.

47. William Fisher. Attribute Based Access Control. — National Institute of Standards and Technology, 2015. — P. 22.

48. Alan H. Karp, etc. From ABAC to ZBAC: The Evolution of Access Control Models. — HP Laboratories, 2009. — P. 21.

49. Bill Parducci, Hal Lockhart. eXtensible Access Control Markup Language (XACML) Version 3.0 Plus Errata 01. — OASIS, 2017. — P. 154.

50. Xin Jin. ATTRIBUTE-BASED ACCESS CONTROL MODELS AND IMPLEMENTATION IN CLOUD INFRASTRUCTURE AS A SERVICE. — THE UNIVERSITY OF TEXAS AT SAN ANTONIO, 2014. — P. 144.

51. 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.

52. 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.

53. Al-Kahtani M. A. Rule-based rbac with negative authorization / M. A. Al-Kahtani, R. Sandhu. — 2004.

54. Marchenko O. Machine learning method for paraphrase identification / O. Marchenko, A. Anisimov, A. Nykonenko. — Springer, 2017.

55. Ульман Д. Основы систем баз данных / Д. Ульман. — М. : Финансы и статистика, 1983. — 336 с.

56. Терейковський І. А. Формування політики безпеки комп'ютерних систем/ І. А. Терейковський // Захист інформації. — 2008. — Т. 10, № 1. — С. 12–22.

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. Давиденко А. М. Використання формальних засобів опису процесів надання повноважень / А. М. Давиденко, О. А. Суліма // Захист інформації. — 2016. — Т. 18. — С. 143–149.

59. Макконнелл Д. Анализ алгоритмов / Д. Макконнелл. — М. : Техносфера, 2009. — 449 с.

60. 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.

61. Валькман Ю. Р. Модельно-параметрическое пространство: теория и применение / Ю. Р. Валькман, В. И. Гриценко, А. Ю. Рыхальский. — К. : Наукова думка, 2012. — 192 с.

62. Грибунин В. Г. Комплексная система защиты информации на предприятии / В. Г. Грибунин. — М. : Издательский центр «Академия», 2009. — 416 с.

63. 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.

64. Левитин А. В. Алгоритмы: введение в разработку и анализ / А. В. Левитин. — М. : Вильямс, 2006. — 576 с.

65. Пентус А. Е. Теория формальных языков / А. Е. Пентус, М. Р. Пентус. — М. : МГУ, 2004. — 80 с.

66. Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков. — К. : Видавнича група BHV, 2009. — 608 с.

67. Гайкович В. Ю. Безопасность электронных банковских систем / В. Ю. Гайкович. — М. : Единая Европа, 1994. — 364 с.

68. 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.

69. Phillips C. E. Security assurance for an rbac/mac security model / C. E. Phillips, S. A. Demurjian, T. C. Ting. — 2003.

70. 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.

71. Герасименко В. А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. / В.А. Герасименко. – М.: Энергоатомиздат, 1994. – 400 с.

72. Грушо А.А., Тимнонина Е.Е. Теоретические основы защиты информации. - М.: Яхтсмен, 1996. - 304 с.

73. Задирака В. К. Методи захисту банківської інформації / Задирака В.К., Олесюк О.С., Недашковський М.О. – К.: Вища шк., 1999. – 261 с.

74. Искусственный интеллект: В 3-х книгах. Кн. 2. Модели и методы: Справочник / под ред. В. Н. Захарова, Э. В. Попова, Д. А. Поспелова, В. Ф. Хорошевского. – М.: Радио и связь, 1990. – 304 с.

75. Корченко О. Г. Системи захисту інформації / О.Г. Корченко. – К.: НАУ, 2004. – 264 с.

76. Критерии оценки защищенности информации в компьютерных системах от несанкционированного доступа : НД ТЗИ 2.5-004-99. – [Введ. 01.07.99].– К.:ДСТСЗИ СБ Украины, 1999. – 38 с.

77. Лукацкий А. Обнаружение атак / А. Лукацкий. – СПб.: БХВ - Петербург, 2001. – 624 с.

78. Матфик С. Механизмы защиты в сетях ЭВМ / С. Матфик ; пер. с англ. – М.: Мир, 1993. – 216с.

79. Молдовян А. А. Криптография / Молдовян А.А., Молдовян Н.А., Советов Б.Я. – СПб.: «Лань», 2000. – 224 с. – (Серия “Учебники для вузов. Специальная литература”)

80. Новиков П. С. Элементы математической логики / П.С. Новиков. – М.: Наука, 1973. – 399 с.

81. Петраков А. В. Основы практической защиты информации : учеб. пособ. / А.В. Петраков А.В. – М.: Радио и связь, 1999. – 368 с.

82. Петров А. А. Компьютерная безопасность. Криптографические методы защиты / А.А. Петров. – М.: ДМК, 2000. – 445 с.

83. Польман Н. Архитектура брандмауэров для сетей предприятия / Н. Польман, Т. Кразес. – М.: Издательский дом «Вильямс», 2003. – 432 с.

84. Расторгуев С. П. Искусство защиты и "раздевания" программ / С.П. Расторгуев, Н.Н. Дмитриевский. – М.: Совмаркет, 1991. – 94 с.

85. Спесивцев А. В. Защита информации в персональных ЭВМ / Спесивцев А. В., Вегнер В. А., Крутиков А. Ю. – М.: Радио и связь; МП 'Веста', 1992. – 192 с.

86. Столингс В. Основы защиты сетей. Приложения и стандарты / В. Столингс. – М.: Издательский дом «Вильямс», 2002. – 432 с.

87. Ferraiolo D. F., Kuhn D. R. (October 1992). "Role Based Access Control". 15th National Computer Security Conference: 554—563.

88. Sandhu R., Coyne E. J., Feinstein H. L., Youman C. E. (August 1996). «Role-Based Access Control Models». IEEE Computer (IEEE Press) 29 (2): 38–47.

89. Editor, CSRC Content. Role Based Access Control - FAQs. csrc.nist.gov (EN-US). Процитовано 2018-04-07.

90. Ravi Sandhu, Qamar Munawer (October 1998). "How to do discretionary access control using roles". 3rd ACM Workshop on Role-Based Access Control: 47—54.

91. Sylvia Osborn, Ravi Sandhu, Qamar Munawer(2000). "Configuring role-based access control to enforce mandatory and discretionary access control policies". ACM Transactions on Information and System Security (TISSEC): 85—106.

92. Systems, Hitachi ID. Beyond Roles: A Practical Approach to Enterprise IAM. hitachi-id.com (en). Процитовано 2018-04-07.

93. Sandhu R., Ferraiolo D.F. and Kuhn D.R. (July 2000). "The NIST Model for Role Based Access Control: Toward a Unified Standard". 5th ACM Workshop Role-Based Access Control: 47—63.

94. Telecommunications Networks. Current Status and Future Trends. Edited by Jesús Hamilton Ortiz. [Електронний ресурс]. – Режим доступа: https://www.intechopen.com/books/telecommunications-networks-current-status-and-future-trends.

95. David., Ferraiolo,; Richard., Kuhn, D. (2007). Role-based access control (вид. 2nd ed). Boston: Artech House. ISBN 9781596931138. OCLC 427509709.

96. N. Nasser, A. Hasswa & H. Hassanein (2006). Handoffs in Fourth Generation Heterogenous Networks, IEEE Communications Magazine vol. 44(10): pp. 96–103.

97. A. Dutta, D. Famolari, S. Das, Y. Ohba, V. Fajardo, K. Taniuchi, R. Lopez & H. Schulzrinne (2008). Media-Independent Pre-Authentication Suppporting Secure

Interdomain Handover Optimization, IEEE Wireless Communications vol. 15(2): 55–64.

98. Badra, M., Urien, P. & Hajjeh, I. (2007). Flexible and fast security solution for wireless LAN, Pervasive and Mobile Computing Journal 3: 1–14.

99. C. Politis, K. Chew, N. Akhtar, M. Georgiades, R. Tafazolli & T. Dagiuklas (2004). Hybrid multilayer mobility management with AAA context transfer capabilities for all-IP networks, IEEE Wireless Communications 11 pp. pp. 76–88.

100. Marin-Lopez, R., Pereniguez, F., Bernal, F. & Gomez, A. (2010). Secure three-party key distribution protocol for fast network access in EAP-based wireless networks, Computer Networks 54: 2651 – 2673.

101. C. de Laat, G. Gross, L. Gommans, J. Vollbrecht & D. Spence (2000). Generic AAA Architecture. IETF RFC 2903.

РОЗДІЛ 2. ПОБУДОВА МОДЕЛЕЙ ДЛЯ РЕАЛІЗАЦІЇ СИСТЕМ РОЗМЕЖУВАННЯ ДОСТУПУ

2.1. Моделі нейронних мереж в задачах захисту систем керування доступом

Сучасні системи керування доступом розглядаються в різних аспектах. Такі аспекти відображають доступ до даних, при цьому, мова йде про доступ до даних, які знаходяться в базах даних, доступ до процесів, якщо мова йде про надання послуг в межах локальних комп'ютерних мереж і т.д. Другий важливий аспект керування доступом тісно пов'язаний з проблемами ідентифікації і автентифікації, які вирішуються з метою розпізнавання з гарантованою достовірністю об'єктів, які претендують на доступ до тих чи інших засобів. Найчастіше процедури ідентифікації та автентифікації пов'язуються з потенційними користувачами відповідних засобів. Третій аспект захисту контролю доступу пов'язаний з проблемами такої організації процесів або окремих систем, які були б недоступні для різного роду впроваджень, перехоплення або інших способів втручання в відповідний об'єкт або процес. В рамках наведених вище аспектів, задачі захисту доступу до об'єктів, що захищаються, вирішуються різними способами і ці способи в тій чи іншій їх модифікації використовуються в різній мірі в кожному з аспектів. Загальні принципи, на яких ґрунтуються відповідні способи, полягають у наступному [1]:

— у використанні деякої таємної інформації, яка доступна тільки обмеженому колу учасників процесу доступу;

— у використанні методів одностороннього перетворення даних або інформації, що захищається, яка може бути відновлена тільки окремими уповноваженими учасниками, процесу доступу;

— у використанні унікальних даних або властивостей, які досить складно повторити, хоча останні не є таємними.

Характерною особливістю систем доступу є те, що останні, як правило, використовуються в тих випадках, коли об'єкти, на роботу з якими вони орієнтовані, передбачається експлуатувати в режимі масового використання

протягом тривалого часу, яке визначається технічними ресурсами засобів, що реалізують відповідні об’єкти. В цьому випадку, виникає проблема, яка визначає необхідність безперервного моніторингу систем керування доступом, з метою забезпечення необхідного рівня безпеки відповідного доступу.

Для вирішення цієї задачі необхідно мати засоби і відповідні методи оцінки такого рівня безпеки.

Друга проблема, яка виникає в зв’язку з необхідністю довготривалої експлуатації систем доступу полягає в тому, що система захисту або засоби захисту таких систем повинні з часом, в залежності від умов роботи системи доступу, які змінюються, забезпечувати їх модифікацію або адаптацію до умов середовища, в якому системи доступу функціонують. Таким середовищем, для системи доступу є процеси та засоби реалізації процесів доступу.

На даний час, системи доступу найчастіше використовуються для керування доступом до систем, які розподілені в просторі. Системи доступу, про які буде йти мова далі, будуть являти собою розподілені в просторі системи доступу, що передбачає наявність розподілених точок входу в систему. Більшість систем, які вимагають обслуговування системами доступу є розподіленими, що призводить до того, що користувачі розосереджені відповідно до розподілу системи. Тому, таку систему можна представити як мережу пов’язаних між собою вузлів. Безумовно, що окремі вузли пов’язані між собою функціонально. Такі функціональні залежності визначаються архітектурою розподіленої системи, функціональною орієнтацією окремих вузлів та іншими характеристиками або особливостями її функціонування. В свою чергу наявність таких зв’язків призводить до того, що порушення безпеки в одному вузлу може призвести до порушення безпеки в інших вузлах. В зв’язку з цим, виникає необхідність в тому, щоб засоби захисту системи доступу були розподілені аналогічно до основної системи, а зв’язки між ними відображали б взаємозалежність в порушенні безпеки між окремими вузлами. Такі взаємозалежності, в ідеальному випадку повинні відображати вплив зменшення рівня безпеки в одному вузлу на рівень безпеки в інших вузлах. При цьому, зв’язки між вузлами засобів захисту системи доступу не обов’язково повинні відображати функціональні зв’язки між

вузлами об’єкта, доступ до яких передбачається захищати. В якості засобів побудови такої мережі пропонується використовувати нейронні мережі. Для того, щоб можна було реалізовувати відповідну мережу необхідно розглянути основні типи відомих нейронних мереж і дослідити їх можливості. Перш за все зазначимо, що для моделювання засобів захисту системи доступу, байдуже які конкретні механізми в кожному вузлу об’єкта доступу використовуються. Наприклад, такими механізмами можуть бути, системи паролів, системи шифрування, які використовують системи управління ключами, моделі доступу до даних, які розмежовують доступ до послуг і ресурсів відповідно до повноважень і т.д. Нейронна модель системи захисту системи доступу до об’єкту, що охороняється, працює з даними, які характеризують наступне:

— факт порушення умов доступу;

— зміна рівня безпеки в кожному окремому вузлі;

— факти вдалою і невдалою атак на систему доступу кожного окремого вузла і інша інформація, яка може бути використана для роботи системи захисту доступу відповідно до основних функцій нейронної мережі.

До основних структурам нейронної мережі слід віднести наступні структури [2]:

— односпрямовані, багаторівневі мережі сигнального типу;

— радіальні нейронні мережі;

— нейронні мережі зі спеціалізованою структурою або спеціалізовані мережі;

— рекурентні мережі;

— рекурентні персептроноподібні мережі.

Односпрямовані, багаторівневі мережі являють собою рівні нейронів, які об’єднуються тільки з нейронами наступного рівня і взаємодіють між собою тільки в одному напрямку. В такій структурі кожен нейрон одного рівня з’єднується своїм виходом зі входом кожного нейрона наступного рівня. Математична модель такої нейронної мережі описує спосіб визначення вихідного сигналу Y_k в залежності від вхідних сигналів, які надходять з виходів нейронів попередніх рівнів, які в свою чергу залежать від вхідних сигналів попередніх рівнів. Для випадку дворівневої нейронної мережі, співвідношення для виходу нейрона Y_k з вихідного рівня запишеться у вигляді [3]:

$$Y_k = f\left(\sum_{i=0}^{k} w_{k_i}^{(2)} f\left(\sum_{j=0}^{N} w_{ij}^{(1)} x_j\right)\right), \qquad (2.1)$$

де індекс k змінюється від 1 до m і визначає кількість нейронів на вихідному рівні, індекс $i = 1,...,k$ визначає кількість нейронів на попередньому рівні, індекс j визначає кількість нейронів першого рівня і визначається $j = 1,...,N$, w_{ij} - вагові коефіцієнти між i і j - рівнями нейронної мережі, f - функція перетворення, яка реалізується нейроном. Формування структури нейронної мережі ще не досить для того, щоб можна було говорити про її використання. Для того щоб можна було в рамках нейронної мережі вирішувати задачі, що плануються, необхідно провести процедури навчання відповідної мережі, які, по суті, налаштовують мережу на вирішення бажаної задачі. Оскільки нейрони визначаються функціями перетворень, які однакові для всіх нейронів мережі і в процесі функціонування мережі змінюватися не можуть, то залишається змінювати ваги w_{ij} вхідних змінних або вхідних векторів таким чином, щоб при вирішенні реальних задач, якщо вхідні змінні коректні по відношенню до мети задачі, то щоб рішення задачі відповідало мети задачі. Наприклад, якщо метою вирішення задачі є задача ідентифікації або розпізнавання образів, що, по суті одне і те саме, то вагові коефіцієнти повинні мати такі значення, при яких результат перетворень залежить тільки від вхідних змінних. Наприклад, якщо проводиться ідентифікація та параметри, які є вхідними змінними, відповідають об’єкту, що ідентифікується, то в результаті роботи мережі видається параметр, який ідентифікує об’єкт як розпізнаний. Якщо параметри відхиляються в допустимих межах, то мережа теж виконує ідентифікацію і об’єкт визнається розпізнаним. Роль нейронної мережі, в цьому випадку, обумовлюється наступними факторами.

Окремі вхідні змінні найчастіше безпосередньо не ідентифікують об’єкт, що розпізнається. Для ідентифікації об’єкта необхідно здійснити перетворення вхідних даних, які в більшості випадків є досить складними.

Другий фактор полягає в тому, що параметри не завжди можуть бути строго однакові у всіх випадках ідентифікації, яка проводиться по відношенню до одного

і того ж об’єкту. Тому, необхідно мати можливість розпізнавати об’єкт з тією чи іншою мірою наближення або мірою точності.

Третій фактор полягає в тому, що в разі неприпустимих відхилень значень параметрів ідентифікації об’єктів, необхідно визначати міру загрози несанкціонованого доступу.

Четвертий фактор полягає в тому, що в процесі функціонування нейронної мережі, можна її адаптувати до параметрів ідентифікації, що змінюються, змінюючи вагові коефіцієнти за результатами, які підтверджують правильність розпізнавання об’єкта. Такі підтвердження формуються на основі додаткових процедур перевірки об’єкта в процесі його роботи з системою за межами системи доступу.

В теорії нейронних мереж розроблено досить багато алгоритмів навчання. Різні типи алгоритмів навчання залежать від класів нейронних мереж, від функцій перетворень та ряду інших чинників, які визначають характер функціонування мережі. Розглянемо один з базових алгоритмів навчання, який називається алгоритмом зворотного поширення [4].

Для випадку дворівневої, односпрямованої мережі функція мети навчання на основі алгоритму зворотного поширення запишеться наступним чином [4]:

$$E(w) = (1/2)\sum_{j=1}^{p}\sum_{s=1}^{m}\left(Y_k^{(j)} - d_k^{(j)}\right)^2, \qquad (2.2)$$

де p - загальна кількість експериментів, що навчають. На якісному рівні можна прийняти, що метою навчання мережі є визначення величин ваг w нейронів на всіх рівнях мережі таким чином, щоб при заданому вхідному векторі $\overline{X}$ отримати на виході мережі значення вихідних сигналів Y_i, які з точністю, що вимагається, відповідали заданим значенням d_i, для $i = 1,2,...,m$. Навчання мережі, при використанні цього алгоритму реалізується в три фази, які перераховані нижче.

Під час першої фази вибираються зразки одного кроку навчання $\overline{X}$ і обчислюються значення сигналів послідовних нейронів мережі. Для даного вектору обчислюються значення вихідних сигналів v_i для нейронів прихованих рівнів, а після цього обчислюється значення вихідного сигналу Y_i, який відповідає

вихідному рівню мережі. Ці обчислення виконуються відповідно до виразу (2.1) і виразу для обчислення v_i:

$$v_i = f\left(\sum_{j=0}^{N} w_{ij}^{(1)} x_j\right). \tag{2.3}$$

На другій фазі виконується мінімізація функції мети (2.2). При прийнятті умови, що функція f є безперервною, найбільш успішним методом вирішення цієї задачі є градієнтний метод, який реалізується відповідно до наступних виразів:

$$w(k+1) = w(k) + \Delta w,$$

де $\Delta w = \eta p(w)$, а η - коефіцієнт навчання, $p(w)$ - напрямок зміни w. Для реалізації градієнтного методу мінімізації необхідно використати стратегію, яка називається алгоритмом зворотного поширення. Цей алгоритм складається з ряду кроків і повторюється для кожного етапу процесу навчання.

На першому кроці описаним вище чином обчислюються значення вихідних сигналів нейронів прихованих рівнів. Крім того, визначаються похідні функції активації в послідовних рівнях нейронної мережі

$$\frac{df\left(u_i^{(1)}\right)}{du_i^{(1)}}, \frac{df\left(u_i^{(2)}\right)}{du_i^{(2)}}, \ldots, \frac{df\left(u_i^{(m)}\right)}{du_i^{(m)}},$$

де m - кількість рівнів мережі.

На другому кроці формується мережа зворотного поширення таким чином. Напрям передачі сигналів в мережі змінюється на протилежний. Функція активації замінюється її похідними. На колишній вихід мережі подається примус, який дорівнює різниці між величиною, яка отримана і величиною, яка вимагається. Для мережі заданої таким чином обчислюються значення відповідних зворотних різниць.

На третьому кроці реалізується зміна ваг на основі даних, які отримані на першому та другому кроці для нормальної мережі та мережі зворотного поширення.

На четвертому кроці процеси, які описані на кроках 1, 2 і 3, необхідно повторювати для інших послідовностей, які навчають. Цей алгоритм повторюється

до тих пір, поки норма градієнта не стане меншою за певну величину ε, яка визначає точність процесу навчання нейронної мережі.

Наступним класом нейронних мереж є радіальні мережі. Найбільш проста радіальна мережа функціонує за принципом багатовимірної інтерполяції, яка реалізує відображення p різних вхідних векторів $X_i\left(i=1,2,...,p\right)$ з N-вимірного вхідного простору в множину дійсних чисел p. Радіальна мережа, в силу цієї обставини має один вихід і p пар для навчання $\left(X_i,d_i\right)$. Базова функція радіальної мережі записується у вигляді:

$$\phi\left(\overline{X}\right)=\phi\left(\left\|X-c\right\|\right)$$

де c - обраний центр, навколо якого розміщуються приховані нейрони. Апроксимуючу функцію для радіальної мережі можна представити у вигляді:

$$F\left(X\right)=\sum_{i=1}^{k}w_i\phi\left(\left\|\overline{X}-c_i\right\|\right), \qquad (2.4)$$

де c_i - множина центрів, $i-1,...,k.$ В цьому випадку, задача апроксимації полягає в такому виборі ваг w_i і у виборі такого числа центрів, щоб функція (2.4) найкращим чином наближалася до точного рішення. Цю проблему можна звести до мінімізації функції мети, яку можна записати таким чином, якщо використовувати евклідову норму:

$$E=\sum_{i=1}^{p}\left[\sum_{j=1}^{k}w_j\phi\left(\left\|X_i-c_i\right\|\right)-d_i\right]^2,$$

де k - кількість радіальних нейронів, p - кількість пар, що навчають, $\left(X_i,d_i\right)$, X_i - вхідний вектор, а d_i - відповідна йому задана величина. Найчастіше використовується радіальна функція у вигляді функції Гауса:

$$\phi\left(X\right)=\phi\left(\left\|\overline{X}-c_i\right\|\right)=\exp\left(-\left(\left\|\overline{X}-c_i\right\|^2\right)/2\sigma_i^2\right),$$

де σ - параметр, який визначається як щільність відповідної функції.

Наступним типом нейронних мереж є мережа зі спеціалізованою структурою. Прикладом такої мережі може служити мережа каскадної кореляції Falhmana. У цій мережі нейрони з’єднуються у вигляді каскаду вагових зв’язків, що розвивається.

Кожен послідовний нейрон зв'язується з вузлами і всіма вже існуючими нейронами. Більш складним прикладом нейронної мережі зі спеціалізованою структурою є мережа Volterry [5]. Ця мережа є динамічною і призначена для нелінійного перетворення послідовності сигналів. Відповідно до визначення ряду Вольтера, вихідний сигнал y генерується відповідно до залежності:

$$y(n) = \sum_{i=1}^{L} w_i x(n-i) + \sum_{i_1=1}^{L} \sum_{i_2=1}^{L} w_{i_1} w_{i_2} x(n-i_1) x(n-i_2) + \\ + \ldots + \sum_{i_1=1}^{L} \ldots \sum_{i_k=1}^{L} w_{i_1 i_2 \ldots i_k} x(n-i_1) x(n-i_2) \ldots x(n-i_k),$$

де x - вхідний сигнал, а ваги $w_i, w_{ij}, \ldots, w_{ijk}$ і т.д. є ядрами Вольтера.

Окремою групою мереж є мережі, в яких використовуються зворотні зв'язки. Такі мережі називаються рекурентними мережами. Зворотні зв'язку будуються з рівня виходів до прихованих рівнів або до вхідного рівня. Якщо вхідну функцію нейрона записати у вигляді:

$$y_i = f(u_i) = f\left(\sum_{j=1}^{N} (w_{ij}, x_j)\right),$$

що визначає стан відповідного нейрона, то в разі використання зворотного зв'язку, зміну стану нейрона можна описати системою диференціальних рівнянь нелінійного типу представлених у вигляді:

$$\Gamma_i \frac{du_i}{dt} = \sum_{j=i \& j=1}^{N} w_{ij} f(u_j) - u_i - b_i, \qquad (2.5)$$

де b_i - значення величини порогу, який відповідає сигналу поляризації $i = (1, \ldots, N)$, Γ_i - постійна величина коефіцієнта, який визначає час затримки сигналу зворотного зв'язку. Стан нейрона обчислюється на основі розв'язання диференціального рівняння (2.5). Опис стану рекурентної мережі, при певному стані можна описати за допомогою функції Ляпунова [6]:

$$E = -\frac{1}{2} \sum_j \sum_{i,j \neq i} w_{ij} y_i y_j + \sum_{i=1}^{N} \frac{1}{R_i} \int_0^{x_i} f_i^{-1}(y_i) dy_i + \sum_{i=1}^{N} b_i y_i$$

Будемо розглядати даний клас мереж як клас, який функціонує подібно до оперативної пам'яті. Типовими представниками таких мереж є:

- мережа Hopfielda;
- мережа Hemminga;

— мережа типу BAM (Bidirectional Associative Memory).

Базовою задачею для асоціативної пам'яті є наступна задача. Асоціативна пам'ять, при подачі на вхід деяких еталонних даних, повинна видати на виході дані, які з усіх даних, які знаходяться в пам'яті, найбільш близькі до даних, поданих на вхід пам'яті. Для визначення відстані або міри близькості між даними, поданими на вхід і даними, які отримані на виході, найчастіше використовуються відстань Хеммінга. Якщо вхідні і вихідні дані представляти у вигляді векторів, в разі бінарних чисел, відстань Хеммінга визначається наступним чином:

$$d_H\left(\overline{y},\overline{d}\right)=\sum_{i=1}^{n}\left[d_i\left(1-y_i\right)+\left(1-d_i\right)y_i\right].$$

Розглянемо особливості мережі Hopfielda. Головною особливістю цієї мережі є те, що вихідні сигнали нейронів одночасно є вхідними сигналами мережі або $x_i(k)=y_i(k-1)$. У класичному варіанті цієї мережі зворотного зв'язку між входом і виходом одного і того ж нейрона не існує, що означає $w_{ii}=0$ і матриця ваг є асиметричною. Для даних мереж функція активації приймається у вигляді:

$$y_i=\operatorname{sgn}\left(\sum_{j=0}^{N}w_{ij}x_j+b_i\right),$$

що означає, що вихідний сигнал нейрона приймає значення ± 1. При використанні ряду еталонів для процесу навчання $\overline{X}(k),k=1,...,p,$ ваги w_{ij} підбираються відповідно до виразу:

$$w_{ij}=\left(1/N\right)\sum_{k=1}^{p}x_i^{(k)}x_j^{(k)}, \tag{2.6}$$

що означає, що ваги визначаються як середня величина від усього ряду еталонів.

Для мереж цього типу, по відношенню до великої кількості еталонів, які використовуються при навчанні, важливим є поняття стабільності асоціативної пам'яті. Це означає, що з урахуванням виразу (2.6), має місце наступне співвідношення між вхідним і вихідним сигналами:

$$y_i^{(l)}-\operatorname{sgn}\left(\left(1/N\right)\sum_{j=o}^{N}\sum_{k=1}^{p}x_i^{(k)}x_j^{(k)}x_j^{(l)}\right)=x_j^{(l)} \tag{2.7}$$

Це означає, що якщо зважену суму входів $i-$го нейрона позначити $u_i^{(l)}$, можна виділити бажану складову $x_i^{(l)}$, а інші складові прийнято називати складовими, які прослуховуються.

Другим типом рекурентних мереж є мережа Hamminga [7]. Ця мережа являє собою трирівневу рекурсивну структуру. Перший рівень мережі являє собою односпрямовані вхідні нейрони з певними значеннями ваг. Другий рівень являє собою нейрони, які з'єднуються зворотними зв'язками за принципом «кожен з кожним». Цей рівень прийнято називати MAXNET. Ваги нейронів на цьому рівні є постійними. Ваги нейронів на рівні MAXNET такі, що зв'язки між різними нейронами є такими, що гасять. Цю мережу можна представити як мережу, функціонування якої складається з трьох фаз. На першій фазі на входи першого рівня подається $N-$елементний вектор $\bar{x}$. В результаті цього на виходах нейронів генеруються сигнали, які ініціюють нейрони другого рівня. На другій фазі починається процес ітерації, який триває до тих пір, поки всі нейрони за винятком одного не досягнуть вихідного сигналу, який дорівнює нулю. Нейрон з ненульовим вихідним сигналом представляє відповідний клас, до якого належить вхідний вектор $\bar{x}$. У третій фазі відповідний нейрон, за допомогою ваг, які з'єднують його з нейронами вихідного рівня, формує на виході нейронів третього вихідного рівня вектор $\bar{y}$, який асоціюється з вхідним вектором $\bar{x}$. Ця мережа являє собою готероасоціативну пам'ять. Підбір ваг для першого рівня цієї мережі здійснюється відповідно до рівняння $w_{ij}^{(1)} = x_j^{(i)}$, для $i = 1,..., p.$ Підбір ваг для вихідного рівня здійснюється відповідно до співвідношення $w_{ji}^{(2)} = y_j^{(i)}$. Функціонування нейронів в наступних рівнях відрізняється від функціонування нейронів вхідного і вихідного рівнів. Значення сигналів вхідного рівня визначаються наступним виразом:

$$y_i = 1 - \left(d_H \left(\overline{x^{(i)}}, x \right) \right) / n.$$

Процес формування сигналів рівня MAXNET є рекурсивним процесом і описується наступним чином:

$$y_i(k) = f\left(y_i(k-1) + \sum_{j \neq i} w_{ij}^{(m)} y_j(k-1)\right).$$

Важливою особливістю цих мереж є велика економія в кількості вагових зв'язків.

Наступним типом мереж, які відносяться до цього класу, є мережі типу BAM (Bidirectional Associative Memory), які запропоновані в роботі [8]. Передача сигналів здійснюється від входу до виходу в обох напрямах. Характер функціонування цієї мережі є синхронним. Це означає, що в одному циклі відбувається передача сигналів від однієї сторони до іншої, при цьому визначаються стани нейронів, до яких надходять сигнали. У наступному циклі сигнали передаються з другої сторони до першої і при цьому визначаються стани нейронів першої сторони. Цей цикл повторюється до тих пір, поки між двома рівнями нейронів не встановиться рівновага. Зрозуміло, що стан нейронів визначається їх вагами. Матриця ваг визначається як матриця кореляції $W = \sum_{i=1}^{m} X_i^T Y_i$. Процес двонаправленого перетворення сигналів можна описати наступною послідовністю:

$$f(x_0, w) = y_1 \to f(y_1, w^T) = x_1 \to f(x_1, w) = y_2 \to f(y_2, w^T) = x_2 \to f(x_2, w) = y_3 \to \ldots \to$$
$$\to f(y_f, w^T) = x_f \to f(x_f, w) = y_{f+1}.$$

В результаті визначаються два значення, які стабілізують стан мережі.

В роботі [9] запропоновано замінити матрицю W матрицею типу $W_f = [WW_y]$ і, при передачі сигналів зі старих X, матрицею $W_b = [W^T W_x]$. Додаткові матриці визначаються відповідно до співвідношень:

$$W_y = \sum_{i=1}^{m} \overline{X_i^T}\,\overline{Y_i} \;;\; W_x = \sum_{i=1}^{m} \overline{Y_i^T}\,\overline{X_i}.$$

Ці матриці сконструйовані таким чином, що їх вплив зникає при нормальному функціонуванні алгоритму навчання і включаються вони тільки при зашумленні процесу відображення. У цьому випадку наступним чином формується матриця додаткових вузлів мережі:

$$T_y = \sum_{j=1}^{m} g_y \overline{y_j^T}\,\overline{y_j} \;;\; T_x = \sum_{j=1}^{m} g_x \overline{x_j^T}\,\overline{x_j}.$$

В цьому випадку рекурентний процес описується наступними виразами:

$$y_1 = f\left(x_0 W + g_y\left(x_0 W_y\right)T_y\right), x_1 = f\left(y_1 W^T + g_x\left(y_1 W_x\right)T_x\right)...$$
$$...y_f = f\left(x_{f-1} W + g_y\left(x_{f-1} W_y\right)T_y\right), x_f = f\left(y_f W^T + g_x\left(y_f W_x\right)T_x\right).$$

Одним з найпростіших способів отримання рекурентної мережі з односпрямованої мережі є додавання зворотних зв'язків до перцептронової мережі, яку називають RMLP (Recurrent Multi Layer Perseptron). Ця мережа є динамічною і характеризується затримками вхідних і вихідних сигналів, які разом формують вхідний вектор мережі. Якщо позначити через u_i суму ваг сигналів i – того нейрона прихованого рівня, а g – суму ваг сигналів вихідних нейронів, то можна записати:

$$u_i = \sum\ w_{ij}^{(1)} x_j;\ v_i = f\left(u_i\right); g = \sum_{i=0}^{k} w_i^{(2)} f\left(u_i\right);\ y = f\left(g\right).$$

Алгоритм навчання такої мережі ґрунтується на використанні наступної функції мети:

$$E\left(k\right) = \left(1/2\right)\left[y\left(k\right) - d\left(k\right)\right]^2$$

Диференціюючи цю функцію можна отримати вираз, який дозволяє обчислити похідну вихідного сигналу $y(k)$ по вазі $w_d^{(2)}$, яка в остаточному вигляді записується:

$$\frac{dy\left(k\right)}{dw_d^{(2)}} = \frac{df\left(g\left(k\right)\right)}{dg\left(k\right)}\left[v_d\left(k\right) + \sum_{i=0}^{k} w_i^{(2)} \frac{df\left(u_i\left(k\right)\right)}{du_i\left(k\right)} \sum_{j=1}^{p} w_{i,j+N}^{(1)} \frac{dy\left(k-p-1+j\right)}{dw_d^{(2)}}\right].$$

Використовуючи вираз цього типу, можна реалізувати градієнтний метод навчання мережі.

2.2. Дослідження параметрів нейронних мереж, що характеризують їх функціональні можливості

Нейронні мережі з різними структурами орієнтовані на вирішення різних завдань [10-13]. Оскільки вирішення задач здійснюється в цілому нейронною мережею, то необхідно розглянути параметри, які характеризують нейронну мережу в цілому. Більшість задач, які вирішуються на основі використання нейронних мереж вимагають формування моделей тих процесів і об'єктів, до яких

такі задачі мають відношення. Оскільки такі засоби моделювання, як нейронні мережі, самі по собі є досить складними, тому вони, в процесі вирішення відповідної задачі можуть впливати не тільки на процес вирішення, а й результати, які одержуються з їх допомогою. Тому необхідно дослідити інтегральні параметри, які характеризують нейронні мережі. Особливо важливими, для вирішення складних задач, є динамічні параметри нейронних мереж, оскільки вони безпосередньо не описуються співвідношенням, які представляють ту чи іншу структуру мережі, а також вони не відображаються функціями перетворень, що реалізують окремі нейрони. До інтегральних параметрам нейронної мережі можна віднести наступні [3]:

- швидкість перетворення вхідних даних;
- пропускна здатність нейронної мережі;
- енергетична функція нейронної мережі;
- точність перетворення нейронної мережі;
- властивість запам’ятовування вхідних даних нейронною мережею;
- стійкість функціонування нейронної мережі;
- стабільність збереження даних, які запам’ятовувалися і т.д.

Розширення переліку інтегральних параметрів нейронної мережі можливо за рахунок розгляду різного класу задач і визначення наступних загальних параметрів мережі, які безпосередньо пов’язані з тією чи іншою задачею. Нейронні мережі являють собою засоби перетворень, які за своєю природою орієнтовані на моделювання процесів перетворення вхідних даних. Нейронна мережа, теоретично, не обмежує розмірності даних, що одночасно подаються на вхід. Проте, швидкість перетворень даних визначається не тільки швидкістю функціональних перетворень послідовності нейронів, які послідовно обробляють конкретний елемент вхідних даних. Справа в тому, що вхідні дані, які подаються на вхід одночасно є величинами взаємопов’язаними і цей взаємозв’язок необхідно враховувати в рамках нейронної мережі при обробці кожного елемента вхідних даних. Відповідно до ідеології нейронної мережі, такий взаємовплив різних нейронів здійснюється за рахунок встановлення ваг зв’язків між різними нейронами. Ця установка

здійснюється в процесі інсталяції в нейронній мережі певних умов, які забезпечували б її функціонування відповідно до алгоритму функціонування, що вимагається. Таким чином, швидкість функціонування визначається часом, який необхідний для реалізації всіх перетворень, що відбуваються в мережі при подачі на входи сукупності вхідних даних. Щоб підкреслити взаємозв'язок між цими даними, будемо говорити, що на вхід подається вхідний вектор даних.

З наведеного вище випливає, що інтегральні оцінки параметрів недоцільно розраховувати детермінованими методами, оскільки, складність такого розрахунку корелює зі складністю нейронної мережі.

Розглянемо параметри і різні особливості мереж та їх елементів, які враховують фактори, що впливають на їх роботу і при цьому, не є для мереж і нейронів базовими. Прикладом такого фактору може служити шум. У цьому випадку потенціал, діючий на вхід нейрона, не може бути представлений дискретною величиною, а представляється як величина ймовірності поточного значення потенціалу з розподілом Гаусса. Тоді, ймовірність досягнення величиною потенціалу значення необхідного для збудження нейрона може бути записана у вигляді [3]:

$$Pi(s_i) = \left(\exp(\beta h_i s_i)\right) / \left(\exp(\beta h_i s_i) + \exp(-\beta h_i s_i)\right),$$

де $s_i = \mathrm{sgn}(h_i), h_i = \langle u_i \rangle - \mathrm{T}_i, \mathrm{T}_i -$ поріг збудження, u_i - поточне значення потенціалу збудження, $\beta = 1/\delta\sqrt{2}, \delta$ - ширина функції збудження, яка представлена функцією розподілу Гауса. Цей вираз можна інтерпретувати як опис динаміки нейрона при наявності шуму.

В процесі функціонування, в нейронній мережі відбуваються зміни, які в цілому описують динаміку функціонування. При цьому, мережа може з часом переходити в стійкі стани, в циклічні стани або стани в часі можуть змінюватися іншим будь-яким чином. Це обумовлено тим, що на нейронну мережу діє ціла низка факторів, які є другорядними, наприклад, шуми, помилки перетворень і т.д. Особливо характерні такі зміни для недетермінованих нейронних мереж. Для опису таких змін зручно використовувати уявлення про фазові траєкторії. Фазова

траєкторія являє собою криву, яка об'єднує послідовні точки стану мережі. Використання фазових траєкторій дозволяє описувати часову еволюцію мережі. У цьому випадку доцільно використовувати поняття перекривання, яке показує міру подібності поточного стану мережі в момент t до μ-го стану мережі, формально це записується в такий спосіб:

$$m\mu(t) = (1/\mathrm{N})\sum_{i=1}^{\mathrm{N}} \xi_i^{\mu} S_i(t), \qquad (2.8)$$

де $S_i(t)$ - стан нейрона в момент t, ξ_i^{μ} - стан того ж нейрона в момент μ.

Один з інтегральних параметрів мережі пов'язаний з поняттям енергетичної функції мережі. Це поняття ґрунтується на аналогіях між нейронними мережами і фізичними об'єктами, функціонування яких теж можна описувати за допомогою нейронних мереж. Прикладом може служити магнетик Ісінга [14]. У разі нейронів $S_i\{-1,+1\}$, енергетична функція записується у вигляді:

$$\mathrm{H}(t) = (1/2)\sum_{i=1}^{\mathrm{N}}\sum_{j=1}^{\mathrm{N}} J_{ij} S_i(t) S_j(t),$$

де J_{ij} – синаптичні зв'язки нейронів S_i і S_j. Для обчислення змін енергії, яка обумовлюється зміною стану нейрона в асинхронної динаміці, приймемо:

$$S_i(t+1) = \mathrm{sgn}[\sum_{j=1}^{\mathrm{N}} J_{ij} S_j(t)] \text{ і } S_i(t+1)[\mathrm{sgn}\sum_{j=1}^{\mathrm{N}} J_{ij} S_j(t)] > 0.$$

Тоді для $\Delta\mathrm{H}$ можна записати:

$$\Delta\mathrm{H}_i = -[S_i(t+1)\sum_{j=1, j\neq 1}^{\mathrm{N}} J_{ij} S_j(t)]$$

Якщо прийняти, що $S_i(t+1) - S_i(t) = \mathrm{H}_i S_i(t+1)$, що означає, що H_i може приймати значення:

$$\left[S_i(t+1) = S_i(t)\right] \longrightarrow (\mathrm{H}_i = 0)$$

$$\left[S_i(t+1) = -S_i(t)\right] \longrightarrow (\mathrm{H}_i = 1)$$

В цьому випадку можна записати:

$$\Delta\mathrm{H}_i = -\mathrm{H}_i S_i(t+1)\sum_{j=1, j=i}^{\mathrm{N}} J_{ij} S_j(t).$$

З цього виразу випливає, що якщо $\Delta\mathrm{H}_i = 0$, то $\mathrm{H}_i = 0$ і $S_i(t+1) = S_i(t)$.

Аналогічно можна розглядати випадок, коли є синхронна динаміка. В цьому випадку, для опису енергетичної функції необхідно використовувати функцію Ляпунова [5]:

$$L(t,t+1)=\sum_{i=1}^{\mathrm{N}}\sum_{j=1}^{\mathrm{N}}J_{ij}S_j(t)S_i(t+1),$$

$$\Delta L=L(t+1,t+2)-L(t,t+1)=\sum_{i=1}^{\mathrm{N}}\left\{S_j(t+2)\sum_{j=1}^{\mathrm{N}}J_{ij}S_i(t+1)-S_j(t)\sum_{j=1}^{\mathrm{N}}J_{ij}S_i(t+1)\right\}.$$

Приймаючи, що синаптичні зв'язки симетричні або $J_{ij}=J_{ji}$, а також що $S_i(t)=\mathrm{H}_iS_i(t+2)$, де

$$\left[S_i(t+2)=S_i(t)\right]\longrightarrow(\mathrm{H}_i=1),$$

$$\left[S_i(t+2)=-S_i(t)\right]\longrightarrow(\mathrm{H}_i=-1),$$

можна співвідношення для ΔL переписати у вигляді:

$$\Delta L=\sum_{i=1}^{\mathrm{N}}(1-\mathrm{H}_i)\mathrm{X}_i,$$

де $\mathrm{X}_i=S_i(t+2)\sum_{j=1}^{\mathrm{N}}J_{ij}S_i(t+1)$. В цьому випадку можна записати, що $L_{\max}=\sum_{i=1}^{\mathrm{N}}\sum_{j=1}^{\mathrm{N}}\left|J_{ij}\right|, L_{\min}=\sum_{i=1}^{\mathrm{N}}\sum_{j=1}^{\mathrm{N}}\left|J_{ij}\right|$.

Одними з важливих інтегральних параметрів нейронної мережі є параметри, які характеризують пам'ять нейронної мережі. Якщо обмежитися динамічними параметрами, що стосуються пам'яті, тоді слід говорити про стабільність пам'яті, яка характеризує величину зміни пам'яті мережі. Це в свою чергу, характеризує величину зміни еталонних зразків, які введені в нейронну мережу в процесі навчання. Розглянемо рекурентну модель Хопфілда з великою кількістю нейронів [15]. Приймемо, що мережа знаходиться в стані {si}, яке відповідає запам'ятовуванню одного зразка, номер якого 1 або $\left\{\xi_i^1\right\}$. Умова стабільності полягає в тому, щоб знак локального поля, яке діє на кожен нейрон, збігався зі знаком цього нейрона -1 або $+1$. Це означає, що має дотримуватися співвідношення $h_is_i>0$ для $i=1,2,...,\mathrm{N}$. Нехай ми досліджуємо стійкість в мережі, яка стосується нейрона 1 або $\xi_I^1=\xi_J^1$. Тоді можна записати співвідношення:

$$h_1 s_1 = h_1 \xi_1^1 = \xi_1^1 (1/\mathrm{N}) \sum_{j=2}^{\mathrm{N}} \xi_1^1 \xi_j^1 \xi_j^i + (1/\mathrm{N}) \sum_{j=2}^{\mathrm{N}} \sum_{\mu=2}^{p} \xi_1^1 \xi_1^\mu \xi_j^\mu \xi_j^i,$$

де виділено складові з першої суми з $\mu = 1$. Пам'ятаючи, що $(\xi_i)^2 = 1$, а $(1/\mathrm{N}) \sum_{j=2}^{\mathrm{N}} (\xi)^2 = (\mathrm{N}-1)/\mathrm{N}$ отримаємо:

$$h_1 \xi_1^1 = \left((\mathrm{N}-1)\mathrm{N}\right) + (1/\mathrm{N}) \sum_{j=2}^{\mathrm{N}} \sum_{\mu=2}^{p} \xi_1^1 \xi_1^\mu \xi_j^\mu \xi^i{}_j.$$

Перша складова відповідає першому еталону. Друга складова пов'язана з усіма іншими еталонами, які були успішно запам'ятовано, назвемо її прослуховуванням і позначимо R. При $\mathrm{N} \to \infty$, перший член дорівнює 1. Для забезпечення стабільності $h_1 \xi_1^1 > 0$, необхідно, щоб другий член був більше - 1. Під знаком суми знаходяться добуток зі значеннями $\xi = -1, +1$, які є випадковими змінними, що не корелюють між собою, оскільки зразки теж між собою не корелюють. У разі, коли $\mathrm{N} \to \infty$, то й $p \to \infty$ і тоді член прослуховування являє собою ряд $(\mathrm{N}-1)(p-1) \approx \mathrm{N}_p$ бітів, які дорівнюють - 1 або + 1. Оскільки прослуховування поводиться як випадкова змінна з гаусовською функцією розподілу, у якої середнє значення дорівнює нулю, а середнє відхилення $\sigma^2 = p/\mathrm{N}$, то для ймовірності значення цієї величини можна записати співвідношення:

$$p\left(h_1 \xi_1^1 > 0\right) = p(-1 < R < \infty) = \left(1/\sqrt{2\pi\sigma^2}\right) \int_{-1}^{\infty} e^{\left(-x^2\right)/2\sigma^2} dx = (1/2)\left[1 + erf\left(\sqrt{\frac{1}{2\sigma^2}}\right)\right].$$ де

$erf(x) \approx 1 - \left(1/x\sqrt{\pi}\right) e^{-x^2}$. Прийнявши $a = p/\mathrm{N} = \sigma^2$, можна записати :

$$\mathrm{P}_{(стаб.еталона)} \approx 1 - \mathrm{N}\sqrt{a/2\pi} e^{(-1)/2a}.$$

Для того, щоб цей вираз був близький до 1, необхідно, щоб другий член був достатньо меншим за 1. Беручи до уваги, що $\mathrm{N} \to \infty$, можна стверджувати, що для виконання цієї умови необхідно щоб $a = 1/2\ln \mathrm{N}$. Отже, умова стабільності виконується, коли $a = P/N$ і не перевищує $a = a_c = 1/\ln N$ або, за умови, коли

максимальна кількість еталонів, які запам'ятовуються в мережі, не перевищує $p_c = a_c \mathrm{N} = \mathrm{N} / 2\ln \mathrm{N}$. Це співвідношення визначає максимальну ємність мережі [15]. З цього випливає, що фактором, що призводить до дестабілізації, є існування інших еталонів, які були запам'ятовано, які представляються складової прослуховування. З викладеного випливає, що, якщо в процесі навчання мережі, перейдено поріг максимальної ємності мережі, тоді це призводить до виникнення нестабільності роботи мережі.

Нейронна мережа за своєю структурою і способом функціонування в деякому наближенні аналогічна фізичним об'єктам, які описуються в статистичній механіки. До таких об'єктів належать феромагнетики, явища намагнічування яких та уявлення про їх структуру близькі до структур нейронів. Наприклад, нейрон може приймати значення +1 та - 1, що відповідає стану магнітних моментів атомів, другим фактором є наявність зовнішнього магнітного поля, яке може впорядкувати орієнтацію магнітних моментів, а щодо нейронних мереж існують зовнішні впливи, які реалізуються в процесі навчання і ці процеси призводять до того, що нейрони займають цілком певні значення +1 або - 1. Це призводить до дослідження можливостей застосування апарату статистичної механіки до опису динаміки нейронних структур. Відображенням динаміки нейронної мережі є опис її еволюції. При використанні для цієї мети методів статистичної механіки, основним засобом для опису еволюційних процесів є імовірнісні засоби. Наприклад, появи чергових змін нейронних мереж описуються ймовірностями їх виникнення. Загалом, ймовірність появи конфігурації мережі $\{s_i\}$ залежить від енергії відповідної конфігурації, про яку вже згадувалося. Ця ймовірність є тим менше, чим вище енергія відповідної організації, оскільки в процесі часової еволюції мережа переходить зі стану з вищої енергією в стан з нижчою енергією. Для нейронної мережі з температурою Т, яка для мережі інтерпретується як рівень переходу з одного стану в інший, можна використовувати канонічне статистичне розкладання і тоді ймовірність виникнення в мережі конфігурації $\{s_i\}$ може бути записана у вигляді:

$$\mathrm{P}_{ey.}\left(\{s_i\}\right)=\left(1/\mathrm{Z}\right)\exp\left[-\left(\mathrm{E}\left(\{s_i\}\right)/\mathrm{T}\right)\right],$$

де індекс *ey* визначає ймовірність в стані рівноваги, Z - нормалізує коефіцієнт, енергія стану мережі $\{s_i\}$ описується співвідношенням:

$$\mathrm{E}\left(\{s_i\}\right)=-\left(1/2\right)\sum_{i,j,i\neq j}J_{ij}S_iS_j$$

Для одного нейрона енергія визначається як $\mathrm{E}=-s_i\,h_i,$ де h_i- потенціали, що надходять нейрону від нейронів пресинаптичних. Кожен нейрон може перебувати в стані +1 або - 1 і сума відповідних ймовірностей дорівнює 1, що запишеться у вигляді:

$$\mathrm{P}_{eд.}\left(\{s_i=1\}\right)+\mathrm{P}_{eд.}\left(\{s_i=-1\}\right)=\left(1/\mathrm{Z}\right)\exp\left(h/\mathrm{T}\right)+\left(1/\mathrm{Z}\right)\exp\left(-h_i/\mathrm{T}\right)=1.$$

Звідки випливає співвідношення:

$$\mathrm{Z}=\exp\left(h_i/\mathrm{T}\right)+\exp\left(-h_i/\mathrm{T}\right)=2\cos\left(h_i/\mathrm{T}\right).$$

В цьому випадку, для статистичного ансамблю можна описати середню енергію для всієї нейронної мережі у вигляді співвідношення:

$$\left\langle \mathrm{E}\right\rangle=\sum_{si}\mathrm{P}_{eд.}\left(\{s_i\}\right)\mathrm{E}\left(\{s_i\}\right)=1/\mathrm{Z}\sum_{\{si\}}\mathrm{E}\left(\{s_i\}\right)\exp\left[-\beta\mathrm{E}\left(\{s_i\}\right)\right]=\frac{\partial}{\partial\beta}\left(\ln\mathrm{Z}\right),$$

де Z – статистична сума всієї нейронної мережі, $\beta=1/\mathrm{T}.$

Розглянемо можливий спосіб опису стану нейронної мережі в момент часу $t+\Delta t,$ якщо відомо стан в момент t. Очевидно, що для використання засобів статистичної механіки, необхідно прийняти, що на певні нейрони діє шум і визначено аналог температури $\mathrm{T}>0$. Імовірність виникнення деякого стану мережі в момент $t+\Delta t,$ будемо позначати $\mathrm{P}_{t+\Delta t}\left(...\{s_i\}...\right)$ і вона залежить від способу обчислення нового стану. Для випадку асинхронної динаміки, новий стан мережі виникає, якщо випадково вибрані i-ті нейрони змінюють свій стан відповідно до співвідношень, які були наведені вище:

$S_i=+1$ з імовірністю $\left[1/2+1/2tgh\left(h_i/\mathrm{T}\right)\right]=\exp\left(\beta h_iS_i\right)/\left(\exp\left(-\beta h_iS_i\right)\right),$

$S_i=-1$ з імовірністю

$$\left[1/2-1/2tgh\left(h_i/\mathrm{T}\right)\right]=\exp\left(-\beta h_i S_i\right)/\left(\exp\left(\beta h_i S_i\right)+\exp\left(-\beta h_i S_i\right)\right).$$

Імовірність того, що в момент $t+\Delta t,$ виникає конфігурація $\{S_i\}$ дорівнює сумі імовірностей того, що i –тий нейрон не змінить свого стану:

$$\left(1/\mathrm{N}\right)\sum_i\left[(1/2)+(1/2)tgh\left(\sum_j\left(J_{ij}S_j\right)/\mathrm{T}\right)\right]\mathrm{P}\left(\{S_i\}\right)$$

і ймовірності, що i –тий нейрон змінить свій стан S_i на $S_i^*=-S_i$:

$$\left(1/\mathrm{N}\right)\sum_i\left[(1/2)+(1/2)tgh\left(\sum_j\left(J_{ij}S_i\right)/\mathrm{T}\right)\right]\mathrm{P}\left(\left\{S_i^*\right\}\right).$$

Таким чином, описані ймовірності дозволяють описати еволюцію мережі в момент $t+\Delta t$ у вигляді:

$$\mathrm{P}_{t+\Delta t}\left(\{S_i\}\right)=\left(1/\mathrm{N}\right)\sum_{i=1}^{\mathrm{N}}\left[(1/2)+(1/2)tgh\left(\sum_j\left(J_{ij}S_j\right)/\mathrm{T}\right)\right]*\left[\mathrm{P}\left(\{S_i\}\right)+\mathrm{P}\left(\{S_i\}\right)\right],$$

де стани S_i и S_i^* описують зворотні стани i -го нейрона і пов’язані між собою таким співвідношенням:

$$\mathrm{P}_{e\partial.}\left(\left\{S_i^*\right\}\right)=\exp\left(-\left(2/\mathrm{T}\right)\sum_j J_{ij}S_iS_j\right)*\mathrm{P}_{e\partial.}\left(\{S_i\}\right).$$

Уявлення про середні поля, що виникли в статистичній механіці, дозволили створити моделі, які описують динамічні процеси в тілах типу магнетиків. В даному випадку розглянемо використання цього поняття для опису моделі нейронної мережі Хопфілда з симетричними зв’язками $J_{ij}=J_{ji}$, в якій записано p еталонних випадкових образів. Як уже згадувалося, ймовірність того, що i -тий нейрон прийме значення 1 записується у вигляді:

$$\mathrm{P}\left(s_i=1\right)=e^{\beta h_i}/\left(e^{\beta h_i}+e^{-\beta h_i}\right).$$

Усереднене значення збудження i -того нейрона

$$\left\langle S_i\right\rangle=\left(+1\right)\mathrm{P}\left(S_i=+1\right)+\left(-1\right)\left[1-\mathrm{P}\left(S_i=1\right)\right].$$

Підставив в це співвідношення попереднє отримаємо:

$$\left\langle S_i\right\rangle=tgh\left(\beta h_i\right).$$

Використовуючи теорію середнього поля, приймемо, що це поле створюється нейронами, значення яких усереднені по флуктуаціях потенціалів. Таке поле

позначимо $\langle h_i \rangle$. Для обчислення $\langle h_i \rangle$ використовуємо залежність $h_i = \sum_{i=1, i \neq j}^{N} J_{ij} S_j$ і вираз для J_{ij}, яке для мережі Хопфілда записується у вигляді:

$$J_{ij} = 1 / N \sum_{\mu=1}^{p} \xi_i^{\mu} \xi_j^{\mu}.$$

В цьому випадку можна записати:

$$\langle h_i \rangle = \sum_{i=1, i \neq j}^{N} J_{ij} \langle S_i \rangle = N^{-1} \sum_{\mu=1}^{p} \left(\sum_{j=1}^{N} \xi_i^{\mu} \xi_j^{\mu} \langle S_i \rangle - \xi_i^{\mu} \xi_j^{\mu} \langle S_i \rangle \right).$$

Приймаючи до уваги співвідношення (2.8), можна для $\langle h_i \rangle$ записати співвідношення:

$$\langle h_i \rangle = \sum_{\mu=1}^{p} \langle m^{\mu} \rangle \xi_i^{\mu} - N^{-1} \sum_{\mu=1}^{p} \xi_i^{\mu} \xi^{\mu}_{j} \langle S_i \rangle.$$

Останній член цього співвідношення, приймаючи до уваги що $\xi_i = \pm 1$, можна записати у вигляді:

$$\left(\langle S_i \rangle \right) / N \sum_{\mu=1}^{N} \left(\xi_i^{\mu} \right)^2 = \left(P / N \right) \langle S_j \rangle.$$

Цей член має інтерпретацію зовнішнього поля h_{ext}, яке створюється всіма нейронами за винятком i-того нейрона. Воно є причиною нестабільності для i-того нейрона. Таким чином, можна записати співвідношення:

$$\langle S_i \rangle = tgh[\beta \sum_{j=1}^{N} J_{ij} \langle S_j \rangle + \beta h_{ext}],$$

яке є рівнянням для середнього поля мережі Хопфілда.

На підставі наведених співвідношень можна вивести формули для обчислення вільної енергії мережі Хопфілда. Доцільність обчислення вільної енергії Хопфилда обумовлена тим, що це дозволяє побудувати гіперплощини з стійкими точками станів мережі, що суттєво при вирішенні задач на моделях нейронних мереж.

2.3. Узагальнення моделі багаторівневої системи доступу

Багаторівневі системи доступу до інформаційних засобів забезпечують можливість реалізації оптимальних процедур здійснення доступу до даних та інших засобів інформаційної системи. Для випадку два ця задача вирішена в [16].

Визначим рівні, що реалізуються у системі розмежування доступу (SNP), особливим чином, пов'язаними з захистом даних.

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

Відповідно визначення для першого рівня 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 надання повноважень. В випадку якщо система розмежування доступу санкціонувала дії користувача, то, коли задача, для розв'язання якої потрібні дані, що мають перший рівень конфіденційності $r_i^{1t}(x_i)$, має надати системі SNP певні дані про задачу Za_i. Такі дані можуть мати різний характер відповідно до рівня конфіденційності даних, за якими звертається задача Za_i. Користувач вводить у систему запит на виконання задачі Za_i але він 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 вона може застосовати частки алгоритмів SNP, що стосуються використання $r_i^{1t}(x_i)$, при цьому використовується тільки програний застосунок який є довіренім та внутрішнім по відношенню до SNP і тільки результат цих перетворень, який уже не має рівня конфіденційності $r_i^{1t}(x_i^*)$, передається задачі і задача активізується використовуючи дані з SNP як вхідними. У зв'язку з цим виникають наступні задачі:

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

– визначення, чи виконується обов'язкова умова шо до того шо отримані вихідні дані в результаті роботи $Az_i[r_i^{1t}(x_i)]$ не характеризуються параметрами конфіденційності $r_i(x_i)$;

– перевірка, чи множина програмних застосунків 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 [16] на основі використання наступних положень.

Положення 2.3.1. Необхідність введення параметру конфіденційності для x_i^* обумовлюється наявністю можливого варіанту використання цих даних, який може призвести до виникнення критичних ситуацій Kr_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 Kr_i, що має негативну інтерпретацію в W_i. У зв'язку з цим необхідно довести, що всі можливі негативні ситуації $Kr_i(W_i)$, 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 2.3.2. Системи IS орієнтовано на обслуговування різних об'єктів, якщо вони потребують використання IS.

Для узагальнення на кількість рівній більш ніж два параметр конфіденційності представленій вектором $r_i(x_i)$ треба замінити на N - мерну матрицю $R(x_i)$.

Розглянемо як зміниться наступне твердження.

Твердження 2.3.1 Множина Kr_i та відповідно множина An_i є обмеженими.

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

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 $R_i^{et} \geq Kr_i(W_i)$. 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: $S_i(W_i) \to S_{i+1}(W_i)$.

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 $d_i(x_{i1},\ldots,x_{ik})$ представляє собою точність цих даних по відношенню до факторів, які вони відображають. Формально це можна описати наступним способом у вигляді співвідношення:

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

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 $R_i(x_i)$.

Таким чином заміна $r_i(x_i)$ на N - мерну матрицю $R(x_i)$, не змінює смисл твердження 2.3.1.

Проаналізуймо використання $R_i^{et}(x_i)$ для розв'язання задачі Za_i з цілю $C_i(Za_i)$, є можливим, якщо виконуються наступні умови:

$$[C_i(Za_i) \neq An_i(W_i)] V [C_i(Za_i) \to \neg An_i(W_i)] \qquad (2.3.1);$$

$$Za_i(x_{i1},\ldots,r_{ij}^t(x_{ij}),\ldots,x_n) \to [(Za_i) \neq An_i(W_i)] \qquad (2.3.2).$$

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 $Kr_i(W_i)$, 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 2.3.2. Система $\{Az_i[R_i(x_i)], \ldots, Az_m[R_m(x_m)]\}$ 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:

$Z_{ai}[x_{is}, \ldots, x_{in}, \ldots, R_i^{gt}(x_i)] \to \{[Ci(Z_{ai})] \to [A_{ni}(W_i)]\}$ якщо умова не виконується, то реалізується перетворення $R_i^{gt}(x_i) \to [R_i^{ht}(x_i^*) \& (h<g)]$ і проводиться перевірка умови (2.3.2). Якщо ця умова не виконується, то відповідне перетворення повторюється з елементом $R_i^{ht}(x_i^*)$ до того часу, поки умова (2.3.2) не стане виконуватися або поки $R_i^{kt}(x_i^*) \to R_i^{ht}(x_i^{n+1})$, 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 (2.3.2) виконується, а система $\{Az_i[R_i(x_i)], \ldots, Az_m[R_m(x_m)]\}$ 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 [17, 18]. 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 $r_i^{lt}(x_i)$ [16].

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 [19-22] 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 $ISUW_i$ 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: $\forall Za_i \exists Za_j[(Za_j \,\&\, Pp_i(W_i)) \to An_i(W_i)]$, 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 $Kr_i(W_i)$ 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 [23, 24]. 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.

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.

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%.

2.4. Розподілені моделі розмежування доступу до інформаційних ресурсів

Для цього побудуємо матриці доступу для різних типів паралельних систем обробки даних:

Конвеєрна і векторна обробка. Основа конвеєрної обробки - відокремити виконання певної операції в кілька етапів (кілька етапів) з передачею даних від одного етапу до наступного. Продуктивність підвищується за рахунок того, що на різних етапах конвеєру виконується кілька операцій одночасно. Конвеєр ефективний тільки

тоді, коли його навантаження близьке до повного, а швидкість доставки нових операндів відповідає максимальній продуктивності конвеєру. Якщо буде затримка, паралельно буде виконуватися менше операцій і загальна продуктивність знизиться. Векторні операції забезпечують ідеальний спосіб повного завантаження обчислювального конвеєру. При виконанні векторної команди одна і та ж операція застосовується до всіх елементів вектору (або найчастіше до відповідних елементів пари векторів). Налаштування конвеєру для певної операції може зайняти деякий час первинної установки, але потім операнди можуть увійти в конвеєр з максимальною швидкістю, дозволеною можливостями пам'яті. Паузи ні у зв'язку з вибором нової команди, ні у зв'язку з визначенням гілки обчислень при умовному переході немає. Таким чином, основним принципом векторних машинних обчислень є виконання якоїсь елементарної операції або комбінації декількох елементарних операцій, які необхідно повторно використовувати до певного блоку даних. Ці операції в оригінальній програмі відповідають невеликим компактним циклам. Матриця доступу конвеєра має векторну структуру MacConv = (r_0, r_1 , … , r_n) де n – глибина конвеєра. Конвеєрна обробка, як найменш продуктивна більш сумісна з однопотоковими механізмами захисту інформації.

Комп'ютер побудований за архітектурою SIMD має SIMDquantityPr=N однакових процесорів, SIMDquantityDFl=N потоків даних і SIMDquantityFlIn=1 один потік команд. Кожен процесор має свою локальну пам'ять. Процесори інтерпретують адреси даних як локальні адреси власної пам'яті або як глобальні адреси. Відповідно маємо множині SIMDmemLoc та SIMDmemGl. Процесори отримують команди з одного і того ж командного центрального контролера і працюють синхронно, а це означає, що на кожному кроці всі процесори виконують однакову команду над даними з власної локальної пам'яті. SIMD машини складаються з великої кількості однакових процесорних елементів з власною пам'яттю. Всі елементи процесора в машині виконують однакову програму. Така архітектура може забезпечити дуже високу продуктивність тільки на тих завданнях, в яких всі процесори можуть виконувати одну і ту ж роботу. Модель обчислення SIMD: одна операція виконується над великим блоком даних, оскільки

паралельність досягається, коли один командний потік відбувається на декількох частинах даних одночасно. Матриця доступу для цієї моделі пам’яті буде двомірною, її розмир визначаються множинами SIMDmemLoc та SIMDmemGl. Формально це можна записати як MacSIMD = f(SIMDmemLoc, SIMDmemGl). З точки зору безпеки обробки інформації механізм захисту може бути однопотоковим, але підчас обробки дані перебувають в не захищеному стані.

Комп'ютер побудований за архітектурою MIMD має MIMDquantityPr=N-процесорів, які самостійно виконують MIMDquantityIn=N-потоків команд та перероблюють SIMDquantityDFl=N потоків даних. Кожен процесор працює під своїм власним потоком команд, тобто комп'ютер MIMD може паралельно запускати абсолютно різні програми. Архітектури MIMD додатково класифікуються відповідно до фізичної організації пам'яті, тобто чи має процесор власну локальну пам'ять і звертається до інших блоків пам'яті за допомогою комутаційної мережі, або комутаційна мережа з'єднує всі процесори з загальною пам'яттю. Матриця доступу для цієї моделі пам’яті залежить від архітектури пам’яті , її розмир визначаються розмірами та типами пам’яті яка використається.

Багатопроцесорні комп’ютері з SIMD-процесорами. Багато сучасних суперкомп'ютерів є багатопроцесорними системами, які використовують векторні процесори або SIMD-процесори в якості обчислювальних елементів. Комп’ютері цього класу мають назву MSIMD. Мови програмування та пов'язані з ними компілятори для машин MSIMD зазвичай надають мовні конструкції, які дозволяють програмісту описувати глобальну паралельність. В рамках кожного завдання компілятор автоматично векторізує відповідні цикли. Машини MSIMD роблять можливим використання кращих з цих двох принципів розпаралелювання: векторні операції для тих частин програми, які підходять для цього, і гнучкість архітектури MIMD для інших частин програми. Але побудова матриці доступу стає не тривіальною науковою задачею.

В першому розділі булі описані моделі розмежування доступу, побудуємо модель Бела – ЛаПадули для типового кластеру УНГ.

Обозначемо множину суб'єктів, для типового кластеру УНГ через StcGr , вона включає множини адміністраторів StcAdGr , локальних користувачів StcLUGr , користувачів віртуальних організацій акредитованих на кластеру StcVoUGr. Формально StcGr = { StcAdGr, StcLUGr, StcVoUGr }.

Множина об'єктів типового кластеру УНГ OtcGR визначається його архітектурою та крім StcGr включає множини ядер керування OtcConNGR обчислювальних ядер OtcCalNGR, внутрешних OtcComInGR та зовнишних OtcComOutGR каналів інтерфейсу, внутрешних OtcAplInGR та грід (зовнишних) OtcAplOutGR процесів, сервісів OtcSerGR, сетів даних OtcCalDateGR.

Множина прав доступу *RGr* для типового кластеру УНГ зберігає класичний характер *RGr* = {*r*, w } де *r* – доступ на читання, *w* – доступ на запис.

Множина рівнів таємності LGr більш обмежена, LGr = {U,SU} де U – відкрита, SU – для службового користування.

Решітка рівнів секретності *ΛGr* відповідає класічної *ΛGr* = ($L, \leq, \cdot, \otimes$).

Множина станів системи VGr –, що представляється у вигляді впорядкованих пар (FGr,MGr), де:

- *FGr*: StcGr∪OtcGR →*LGr* – функція рівнів таємності, яка ставить у відповідність кожному об'єкту і суб'єкту в системі певний рівень таємності;
- *MGr* – матриця поточних прав доступу.

Система ΣGr = (v_0, *RGr*, *TGr*) у моделі Бела – ЛаПадули складається з наступних елементів:

v_0 – початковий стан системи;

RGr – множина прав доступу;

$TGr : V \times RGr \rightarrow V$ – функція переходу, яка у ході виконання запитів переводить систему із одного стану у інший.

Визначення безпечного стану:

Стан *v* називається досяжним у системі ΣGr = (v_0, *RGr*, *TGr*), якщо існує послідовність $\{(r_0, v_0), ..., (r_{n-1}, v_{n-1}), (r_n, v_n)\}: T(r_i, v_i) = v_i + 1 \forall\ i = 0, n-1$. Початковий стан v_0 є досяжним за визначенням.

Відповідно до основної теоремі безпеки Бела — ЛаПадули:

Система $\Sigma Gr = (v_0, RGr, TGr)$ безпечна тоді, і тільки тоді, коли виконані наступні умови:

– початковий стан v_0 є безпечним.

– для будь-якого стану v, який досяжний з v_0 шляхом застосування скінченної послідовності запитів з RGr, таких, що $TGr(v,r)=v^*$, $v=(FGr, MGr)$ і $v^*=(FGr^*, MGr^*)$, для $\forall s \epsilon StcGr, \forall o \epsilon OtcGr$ виконані умови:

- Якщо $r \in MGr^*[s, o]$ і $r \notin MGr\ [s, o]$, то $F^*(o) \leq F^*(s)$
- Якщо $r \in MGr\ [s, o]$ і $FGr^*(s) < FGr^*(o)$, то $r \notin MGr^*[s, o]$
- Якщо $w \in MGr^*[s, o]$ і $w \notin MGr\ [s, o]$, то $FGr^*(s) \leq FGr^*(o)$
- Якщо $w \in MGr\ [s, o]$ і $FGr^*(o) < FGr^*(s)$, то $w \notin MGr^*[s, o]$.

Визначимо відповідні множині для типового кластеру УНГ Україні:

Множина адміністраторів StcAdGr = {AdmMain, AdmSec, AdmMen } , де AdmMain – системній адміністратор, AdmSec –адміністратор безпеки, AdmMen – менеджер грід сайту.

Множина локальних користувачів StcLUGr = $\{Us_0, Us_1, \dots, Us_q\}$ для різних кластерів q варіативна від 3 до 20 користувачів.

Множина користувачів віртуальних організацій акредитованих на кластеру StcVoUGr = $\{VoUs_0, VoUs_1, \dots, VoUs_l\}$ включає підмножині користувачів віртуальних організацій, для різних кластерів l варіативна від 3 до 8 віртуальних організацій:

$VoUs_0 = \{Us_{Vo0}, Us_{Vo1}, \dots, Us_{Voj0}\}$

$VoUs_1 = \{Us_{Vo0}, Us_{Vo1}, \dots, Us_{Voj1}\}$

. . .

$VoUs_l = \{Us_{Vo0}, Us_{Vo1}, \dots, Us_{Vojl}\}$

де $J=(j_0, j_1, j_l)$ масив визначаючий кількість користувачів в j віртуальної організації.

Оскільки StcGr = { StcAdGr, StcLUGr, StcVoUGr }, StcGr можна привести к вигляду матриці нерегулярного типу:

$$StcGr=\begin{bmatrix} AdmMain, & AdmSec, & AdmMen \\ Us_0, & Us_1, \ \dots, & Us_q \\ Us_{Vo0}, & Us_{Vo1}, \ \dots, & Us_{Voj0} \\ Us_{Vo0}, & Us_{Vo1}, \ \dots, & Us_{Voj1} \\ & . \quad . \quad . & \\ Us_{Vo0}, & Us_{Vo1}, \ \dots, & Us_{Vojl} \end{bmatrix}. \qquad (2.4.1)$$

Множина ядер керування:

OtcConNGR = {$Prcont_0$, $Prcont_1$, … , $Prcont_k$ } зазвичай к=8 відповідно до кількості ядер на керуючий ноде.

Множина обчислювальних ядер:

OtcCalNGR = {$Prcal_0$, $Prcal_1$, … , $Prcal_e$ } для УНГ значення е має діапазон [24,400] для EGI відповідно max (e) = 4000.

Множина внутрішніх каналів інтерфейсу:

OtcComInGR = {$Prchanin_0$, $Prchanin_1$, … , $Prchanin_c$ } в випадку infiniband c = 10000.

Множина зовнішніх каналів інтерфейсу:

OtcComOutGR = {$Prchanout_0$, $Prchanout_1$, … , $Prchanout_b$ } в випадку Gigabit internet b = 10000.

Множина внутрішніх процесів:

OtcAplInGR = {$AplIn_0$, $AplIn_1$, … , $AplIn_e$ } від 0 до кількості обчислювальних ядер ядер в кластері.

Множина грід (зовнишних) процесів:

OtcAplOutGR = {$AplOut_0$, $AplOut_1$, … , $AplOut_e$ } від 0 до кількості обчислювальних ядер в кластері.

Множина сервісів:

OtcSerGR = {Ser_0, Ser_1, … , Ser_g } від 0 до кількості обчислювальних ядер ядер в кластері.

Множина сетів даних:

OtcCalDateGR= {$CalDate_0$, $CalDate_1$, … , $CalDate_g$ } від 1 до кількості обчислювальних ядер в кластері.

Відповідно OtcGR можна привести к вигляду матриці нерегулярного типу:

$$OtcGR=\begin{bmatrix} Prcont_0, & Prcont_1, & \dots, & Prcont_k \\ Prcal_0, & Prcal_1, & \dots, & Prcal_e \\ Prchanin_0, & Prchanin_1, & \dots, & Prchanin_c \\ Prchanout_0, & Prchanout_1, & \dots, & Prchanout_b \\ AplIn_0, & AplIn_1, & \dots, & AplIn_e \\ AplOut_0, & AplOut_1, & \dots, & AplOut_e \\ Ser_0, & Ser_1, & \dots, & Ser_g \\ CalDate_0, & CalDate_1, & \dots, & CalDate_g \end{bmatrix}. \quad (2.4.2)$$

Такім чином, множина суб'єктів StcGr відповідно формулі (2.4.1.) має нерегулярну структуру , а для оцінки її розмірності V_{StcGr} можна запропонувати наступне співвідношення $\max(V_{StcGr})= \Sigma (3,q,l*\max(J))$.

Відповідно для наведених даних для УНГ це буде $\max(V_{StcGr})=3+20+8*20 = 163$.

Оцінімо розмірність множині об'єктів типового кластеру УНГ OtcGR відповідно формулі (2.4.2.) має нерегулярну структуру , а для оцінки її розмірності V_{OtcGr} можна запропонувати наступне співвідношення

$\max(V_{OtcGr})=\Sigma (k,e,c,b,e,e,g,g) = k+c+b+3e+2g$

Відповідно для наведених даних для УНГ це буде $\max(V_{OtcGr})=8+10000+10000+3*24+2*24 = 20128$.

Розмірність матриці прав доступу множина суб'єктів до множині об'єктів типового кластеру УНГ має відповідно величину 3 280 864. Відповідно для EGI розмірність матриці прав доступу може звеличитися на три порядки.

Таким чином при класичному підході ми маємо ситуацію колі програмний застосунок диспетчер розмежування доступу має одночасно аналізувати більш трьох мільйонів або при рольовому маємо сформувати мільйоні підматриц доступу

та забезпечити їх онлайн синхронізацію. В обох випадках виникають затримки $t_{Zai}(R_i^t)$ пов'язанні з очікуванням задачею Za_i даних $R_i^t(x_i)$. Для зменшення часу затримки $t_{Zai}(R_i^t)$ сформуємо матрицю доступу структура якої відповідає OtcGR. Введемо для цього поняття декомпозиції матриці розмежування доступу.

Визначення 2.4.1 Під декомпозицією $Dec_i(Md)$ будем розуміти процес розділення матриці розмежування доступу Md на підматриці Md_{prj} кожна із котрих включає підмножину прав доступу окремого обчислювального процесу.

Відповідно задачу декомпозиції формально можна написати як

$Dec_i(Md)=\{ Md_{pr0} , Md_{pr1} , \dots , Md_{pry}\}$ при умові $\min(t_{Zai}(R_i^t))$.

Умова $\min(t_{Zai}(R_i^t))$ визначає що структура підматриц розмежування доступу не може бути довільною.

Умова 2.4.1 Для задовільнення умові $\min(t_{Zai}(R_i^t))$ мера близькості ξ_{mpr} множин $\{ Md_{pr0} , Md_{pr1} , \dots , Md_{pry}\}$ та $\{Prcal_0, Prcal_1, \dots , Prcal_e \}$ має бути максимальною.

Інтуїтивно зрозуміло що при цьому y=e але ще залишається проблема розмірності підматриц Md_{prj} . Вирішення цього питання прямо пов'язано со структурою множин OtcAplInGR та OtcAplInGR і здійснюється окремо для кожной розподіленої системі обробки інформаційного ресурсу.

2.5. Побудова методу оцінки рівня безпеки системи розмежування

Оскільки необхідність у реалізації доступу в рамках комп'ютерних мереж досить велика, то й розмаїтість варіантів його реалізації досить широке [25-33]. Неминучою характеристикою будь-яких засобів доступу є їх безпека. Забезпечується цей параметр засобами захисту доступу. Для введення визначеності в цих міркуваннях про рівень безпеки системи доступу розглянуто наступні визначення, які використані в межах даної роботи і які носять робочий характер.

Визначення 2.5.1. Оцінка рівня безпеки системи доступу буде називатися абсолютної, якщо вона визначає можливість недопущення несанкціонованих змін

в об’єкті доступу, ініційованих з боку користувача незалежно від параметрів, якими користувач характеризується стосовно об’єкта доступу U^a.

Визначення 2.5.2. Оцінка рівня безпеки системи доступу SD буде називатися персональною, якщо вона визначає можливість недопущення несанкціонованих змін параметрів користувача, таким чином, який з погляду користувача є неприпустимим U^p.

Визначення 2.5.3. Оцінка рівня безпеки SD буде називатися відносною, якщо вона визначає можливість несанкціонованого впливу привілейованого користувача на рівень відносної безпеки іншого активного або потенційного користувача U^o.

Введемо наступні параметри, що характеризують кожний з наведених вище типів оцінок рівня безпеки системи доступу.

Оцінка абсолютного рівня безпеки системи доступу U^a характеризується або залежить від наступних параметрів: від рівня захищеності індивідуальних або окремих елементів об’єкта доступу h^p; від кількості відомих загроз, які присутні в об’єкті доступу і можуть використовуватися атаками для несанкціонованого втручання в роботу системи, що становить об’єкт доступу h^y; від кількості зв’язків із зовнішнім оточенням, які реалізуються каналами, що не проходять або не пов’язані із системою доступу h^v; від зовнішньої активності об’єкта доступу стосовно навколишнього середовища h^a; від функціонального завантаження об'єкта доступу задачами, які пов'язані з наданням доступу до системи і пов'язані з іншими задачами, які розв'язуються в рамках інформаційних засобів об'єкта доступу, що будемо позначати h^z. У загальному вигляді, така залежність буде описуватися співвідношенням:

$$U^a = f(h^p, h^y, h^v, h^a, h^z).$$

Параметр h^p визначається наступними особливостями: кількістю використовуваних персональних засобів захисту окремих компонентів об'єкта захисту, наприклад, оперативної пам'яті, постійної пам'яті, процесорних елементів і т.п., при цьому приймемо, що окремий елемент об'єкта захисту володіє хоча б

одним засобом захисту (ξ^k); певним чином градуйовані рівні захищеності, які можуть бути забезпечені окремим засобом захисту, таке градуювання рівня захищеності одного елемента об'єкта захисту носить експертний характер і може встановлюватися для кожного засобу захисту на основі оцінок можливості подолання окремих засобів захисту (ξ^g); взаємозалежностями між окремими засобами захисту, які обумовлюються взаємозалежними процесами функціонування окремих елементів об'єкта захисту (ξ^s). Отже вище згадане формальне напишемо в вигляді співвідношення: $h^p = \phi_p(\xi^k, \xi^g, \xi^s)$.

Аналіз властивостей ξ^k, ξ^g і ξ^s показує, що h^p не описується аналітичною функцією, а являє собою залежність від ξ^k, ξ^g і ξ^s комбінаційного характеру. Це означає, що залежність між h^p і ξ^k, ξ^g та ξ^s описується деяким алгоритмом, що дозволяє, незважаючи на те, що не є традиційним чисельним алгоритмом, визначити деяку відносну величину рівня персональної захищеності h^p.

Величина кількості загроз h^y не може однозначно відображати свій вплив на рівень захищеності окремих елементів в силу наступних причин: оскільки тип загрози пов'язаний з певним типом атак, то в цьому сенсі кожна з загроз є специфічною, крім того специфіка загрози визначається типом елемента об'єкта доступу $OD\,(\xi^e)$; кожна з загроз може мати власну величину активності, яка визначається частотою використання відповідної загрози атаками успішними та не успішними (ξ^a); загрози із часом можуть змінювати свою видимість стосовно системи захисту, яка орієнтована на обслуговування об'єкта доступу ξ^v.

Запишемо в загальному виді залежність h^y від перерахованих параметрів $h^y = \phi_y(\xi^e, \xi^a, \xi^v)$. У результаті аналізу системи захисту OD, можна показати що параметр h^y описується наступним співвідношенням: $h^y = \sum_{i=1}^{n}(\xi_i^e + \xi_i^a) + \xi^v / \Delta t$.

Логічні канали являють собою всі доступні можливості передачі несанкціонованих даних в OD або ж санкціонованих фрагментів програм. До таких

каналів, насамперед, відносяться канали реалізовані Інтернет-сервісом і, в першу чергу, електронною поштою. Такого типу канали є явними, будемо позначати їх змінною ξ^H. Крім видимих каналів в OD існують невидимі канали. Рівень небезпеки, який створюють такі канали будемо позначати змінною ξ^η. Невидимі канали створюються засобами VPN та можуть формуватися легальними користувачами в періоди зміни їхнього статусу системою захисту з легального стану в нелегальне і т.п. Для h^v виконується наступне співвідношення $h^v = \sum_{i=1}^{n} \xi_i^H + \sum_{j=1}^{m} \xi_j^\eta$.

Активність OD стосовно зовнішнього середовища визначається цілим рядом факторів: кількістю користувачів, яких обслуговує система використовуючи систему захисту доступу; кількістю вихідних транзакцій, які ініціює система OD; інтенсивністю технологічного забезпечення процесу функціонування фрагмента загальної мережі Інтернет, якщо OD функціонує в її рамках і іншими факторами прояву факту своєї присутності в загальній мережі Інтернет. Ці параметри формуються і визначаються системними засобами OD та у рамках параметра h^a здійснюється підсумовування їхніх середніх значень.

Параметр функціонального навантаження h^z OD, як і попередній параметр, визначається системними засобами OD, а змінні, які його описують відображають особливості його функціонування, які пов'язані з рівнем безпеки OD. До таких особливостей можна віднести: перезавантаження системних засобів, що сприяє полегшенню рішення задач несанкціонованого проникнення в OD сторонніх фрагментів; перезавантаження пам'яті, що може приводити до втрати санкціонованих даних і ціла низка інших особливостей.

Можливості системи захисту доступу значною мірою залежать від базових компонентів, на основі яких така система реалізується. Інтегральною характеристикою системи захисту є забезпечення оптимального рівня безпеки об'єкта доступу OD. Оптимальність, як правило, припускає існування критерію оптимальності або ряду критеріїв оптимальності, що визначає багатокритеріальну оптимізацію. Коректний вибір одного критерію для рішення задачі оптимізації

можливий у тих випадках, коли фактори задачі, що впливають на результат рішення, можуть у певному змісті погоджуватися з обраним критерієм.

Таким чином метод абсолютної оцінки рівня безпеки системи розмежування визначено в п’яти кроках. Відповідно до формули визначення оцінки абсолютного рівня безпеки системи доступу U^a:

1. Перший крок. Обчислення рівня захищеності індивідуальних або окремих елементів об'єкта доступу h^p.

2. Другий крок. Обчислення кількості відомих загроз, які присутні в об'єкті доступу і можуть використовуватися атаками для несанкціонованого втручання в роботу системи, що становить об'єкт доступу h^y.

3. Третій крок. Обчислення кількості зв’язків із зовнішнім оточенням, які реалізуються каналами, що не проходять або не пов'язані із системою доступу h^v.

4. Четвертий крок. Обчислення зовнішньої активності об'єкта доступу стосовно навколишнього середовища h^a.

5. П’ятий крок. Обчислення функціонального завантаження об'єкта доступу задачами, які пов'язані з наданням доступу до системи і пов'язані з іншими задачами, які розв'язуються в рамках інформаційних засобів об'єкта доступу, що будемо позначати h^z.

2.6. Висновки до другого розділу

У другому розділі наведені необхідні теоретичні особливості нейронних моделей і обрані узагальнені ознаки класифікації нейронних мереж для їх подальшого аналізу. Для введення визначеності в міркуваннях про рівень безпеки системи доступу розглянуто визначення абсолютної, персональної та відносної оцінки рівня безпеки системи розмежування доступу.

Удосконалено метод аналізу системи розмежування доступу, шляхом консолідації оцінки рівня захищеності індивідуальних елементів об'єкта доступу, множини загроз, множини зав’язків із зовнішнім оточенням, функціонального завантаження об'єкта доступу та параметру навантаження обчислювальних ресурсів.

Список використаних джерел до другого розділу

1. Ричард Э. Смит Аутентификация: от паролей до открытых ключей / Э. Смит Ричард ; пер. с англ. – М.: Издательский дом “Вильямс”, 2002. – 432с.

2. Яфраков М.Ф. Особенности комплексного подхода к нейрокомпьютингу / М.Ф. Яфраков, Л.И. Корчагина // Приборостроение. – Известия вузов, 1997. – Т.40. – № 4.

3. Mc Culloch W.S., Pitts W. A logical calculus of the ideas immanent in nervous activity. Bulletin of Mathematical Biophysics, 5, 115-133, 1943.

4. Rosenblatt F. Principles of Neurodinamics. - New York: Spartan Books, 1992.

5. Rugh W. Nonlinear systems a Volterra approach. J. Hopkins Press, New York 1981.

6. Анин Б. Ю. Защита компьютерной информации / Б.Ю. Анин. – СПб.: БХВ-Петербург, 2000. – 384 с.

7. Lippmann R. An introduction to computing with neural nets. IEEE ASSP Magazine, April, 1987, pp. 4-22.

8. Kosko B. Bidirectional associative memories. IEEE Trans. Systems, Man and Cybernetics, 1988, v.18 p.49-60.

9. Бендат Дж Прикладной анализ случайных данных / Дж. Бендат, А. Пирсол. – М.: Мир, 1989. – 540 с.

10. Давиденко А. Н. Исследование параметров нейронных сетей характеризирующих их функциональные возможности / А.Н. Давиденко // Збірник наукових праць Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова. – К.: ІПМЕ ім. Г.Є. Пухова НАНУ, 2006. – Вип. 37. – С. 118-126.

11. Давиденко А. Н. Исследование эффективности применения вероятности применения вероятностных нейронных сетей для решения задачи аутентификации пользователя компьютерных систем / А.Н. Давиденко, Е.А Высоцкая // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: зб. наук. пр. – К., 2004. – Вип. 9. – С. 103-110.

12. А. Н. Давиденко, «Исследование методов обучения нейронных сетей для решения задач противодействия атакам на систему управления доступом», Збірник наукових праць інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Вип. 40, С. 114-122, 2007.

13. А. Н. Давиденко, «Расширение теоретических возможностей математических моделей нейронных сетей обуславливаемых их использованием для решения задач защиты систем доступа», Збірник наукових праць інституту проблем моделюваня в енергетиці ім. Г.Є. Пухова НАН України, Вип. 45, С. 112-115, 2008.

14. Абалмазов Э. И. Методы и инженерно-технические средства противодействия информационным угрозам / Э.И. Абалмазов. – М.: Гротек, 1997. – 248 с.

15. Hopfield J., Tomk D. Neural computations of decisions in optimization problems. Biological Cybernetics, 1985, v.52, pp. 141-152.

16. Суліма О. А. Модель багаторівневої системи доступу / О. А. Суліма // Безпека інформації. — 2017. — Т. 23. — С. 123–130.

17. Валькман Ю. Р. Модельно-параметрическое пространство: теория и применение / Ю. Р. Валькман, В. И. Гриценко, А. Ю. Рыхальский. — К. : Наукова думка, 2012. — 192 с.

18. Аляев Ю. А. Дискретная математика и математическая логика / Ю. А. Аляев, С. Ф. Тюрин. — М. : Финансы и статистика, 2006. — 368 с.

19. A. Davydenko, «Formalization level of abstraction of state information resourses access systems», Scientific letters of academic society of Michel Baludansky, vol.4, no. 1, pp. 35-38, 2016.

20. А. Н. Давиденко, «Математическое моделирование систем и средств защиты критической информации», Збірник наукових праць інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Вип. 4, С. 109-113, 1998.

21. А. Н. Давиденко, «Анализ критериев безопасной обработки информации в КС», Моделювання та інформаційні технології. Зб. наук. праць, Вип. 3, С. 155-160, 1999.

22. А. Н. Давиденко, «Организационные и технологические проблемы криптографической защиты», Моделювання та інформаційні технології. Зб. наук. праць, Вип. 4, С. 10-14, 1999.

23. Левитин А. В. Алгоритмы: введение в разработку и анализ / А. В. Левитин. — М. : Вильямс, 2006. — 576 с.

24. Пентус А. Е. Теория формальных языков / А. Е. Пентус, М. Р. Пентус. — М. : МГУ, 2004. — 80 с.

25. А. Н. Давиденко, «Вероятностная оценка надежности реализации функций защиты информации», Моделювання та інформаційні технології. Зб. наук. праць, Вип. 14, С. 64-70, 2002.

26. А. Н. Давиденко, «Исследование возможностей стандартов безопасности информации», Збірник наукових праць інституту проблем моделювання в енергетиці ім. Г.Є. Пу¬хо¬ва НАН України, Вип. 15, С. 118-122, 2002.

27. А. Н. Давиденко, «Базовые требования к методологии построения угроз для информации с ограниченным доступом в автоматизированных системах», Збірник наукових праць інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Вип. 17, С. 150-154, 2002.

28. А. Н. Давиденко, «Проблемы анализа и моделирования национальных и международных критериев оценки безопасности информации», Збірник наукових праць інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Вип. 18, С. 171-175, 2002.

29. А. Н. Давиденко, «Анализ средств защиты баз данных», Моделювання та інформаційні технології. Зб. наук. праць, Вип. 20, С. 137-141, 2003.

30. А. Н. Давиденко, «Использование ИТ – технологий при автоматизации процесса управления документами», Збірник наукових праць інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Вип. 20, С. 142-147, 2003.

31. А. М. Давиденко, «Проблеми обробки документів за допомогою офісних засобів в аспекті безпеки інформаційного обміну», Збірник наукових праць інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Вип. 21, С. 94-99, 2003.

32. А. Н. Давиденко, «Анализ основных информационных компонент систем доступа», Моделювання та інформаційні технології. Зб. наук. праць, Вип. 59, С.11-20, 2011.

33. А. Н. Давиденко, «Исследование взаимосвязей между семантическими параметрами для области безопасности систем доступа», Моделювання та інформаційні технології. Зб. наук. праць, Вип. 78, С.21-30, 2017.

РОЗДІЛ 3. НАВЧАННЯ НЕЙРОННИХ МОДЕЛЕЙ ЗАСОБІВ ЗАХИСТУ СИСТЕМ ДОСТУПУ

3.1. Теоретичні особливості методів навчання нейронних моделей

Однією з важливих особливостей системи доступу є те, що вона володіє односторонньою персоналізацією. Це означає, що система доступу, що представляє собою засіб зв'язку між мережею і зовнішнім середовищем, з одного боку, орієнтована на певні особливості внутрішнього середовища, яку представляє собою мережу, а з іншого боку, повинна забезпечувати досить універсальні можливості доступу до мережі від зовнішніх споживачів, якими можуть бути окремі користувачі, хости або інші транзакції тих чи інших пакетів.

Другою особливістю системи доступу є рішення нею завдань забезпечення безпечного доступу до внутрішнього середовища. У зв'язку з цим, система доступу повинна мати можливість розпізнавати ситуації, які пов'язані з потенційною небезпекою. Таке розпізнавання може ґрунтуватися на основі наступних підходів [1]:

— на основі ідентифікації зовнішнього агента, який звертається до системи;

— на основі розпізнання небезпеки, яку уособлює агент або є її носієм;

— на підставі формування припущень про міру потенційної небезпеки, носієм, якій може бути визначений агент, який звертається до системи.

Третьою особливістю систем доступу є рішення задач протидії до небезпек, які виявлені в рамках системи доступу.

Розглянемо більш детально другу особливість. У більшості випадків, системи доступу асоціюються з реалізацією першого підходу до організації її роботи. У зв'язку з цим, в рамках системи такого типу існують система ідентифікаторів зовнішніх агентів, які можуть звертатися до системи. Тому виявляється необхідним взаємодія агента з системою реалізовувати через такі засоби доступу, яким необхідні наступні етапи [1]:

— етап реєстрації потенційного агента;

— етап взаємодії агента з системою;

— етап взаємодії системи з агентом.

Перші два етапи є обов'язковими, оскільки без реєстрації агента в системі, останній, в зв'язку з вимогами безпеки, не буде допущений до системи. Третій етап є додатковим і, в першу чергу, пов'язаний із забезпеченням більш високого рівня безпеки системи. Як правило, цей етап реалізується по відношенню до агента, який володіє зареєстрованим каналом доступу до мережі. Відповідна реєстрація реалізується на першому етапі реєстрації агента. Відомі протоколи безпеки [2], при реалізації яких функції третього етапу передбачені в рамках процедури реєстрації агента.

Другий і третій підходи більш характерні для інших засобів захисту локальної мережі. При цьому, всі засоби безпеки взаємодіють між собою при вирішенні завдань забезпечення безпеки системи доступу. В цьому випадку, таке завдання є однією з основних ініціаторів таких взаємодій.

Система доступу, яка розглядається в даній роботі, орієнтована на роботу з агентами, які представляють собою окремих користувачів ресурсами системи, які в свою чергу являють собою інформаційні засоби або обчислювальні засоби, необхідні для вирішення окремих завдань. Незалежно від того, що при реєстрації чергового користувача, останній надає про себе і характер своєї роботи та інформацію, яка необхідна для його якісного забезпечення інформаційної послугою, яку надає мережа. В процесі роботи системи можуть виникати проблеми з поточною ідентифікацією користувача, якщо характер його роботи з інформаційною системою змінюється, або, якщо захисне спорядження не може в силу різних причин ідентифікувати відповідного користувача. Асортимент причин, за якими система ідентифікації може ідентифікувати користувача досить широкий і він може відображати природні процеси, які відбуваються при спілкуванні користувача з системою. Оскільки ці причини можуть НЕ визначатися небезпеками, які існують по відношенні до системи, то виникає проблема адаптації системи ідентифікації і аутентифікації до постійно

змінюваних параметрах легального користувача. В даному випадку, обмежимося підсистемою захисту доступу, яка вирішує завдання ідентифікації і аутентифікації користувачів [3]. Очевидно, що і для інших підсистем системи доступу, в рамках яких вирішується завдання захисту доступу, теж можна використовувати методи захисту, які будемо досліджувати на прикладі вирішення завдань захисту доступу в рамках підсистем ідентифікації і аутентифікації.

Найбільш поширені методи захисту доступу в рамках підсистем ідентифікації ґрунтуються на використанні профілів користувача. Такі профілі в процесі роботи можуть модифікуватися і, при цьому, залишатися відповідними реальному користувачеві. Це означає, що система ідентифікації повинна в процесі її експлуатацій навчитися розпізнаванню змінюваних значень параметрів і самих параметрів, що характеризують легального користувача. Найбільш підходящим засобом для побудови систем, які володіють відповідними можливостями, є нейронні мережі [4].

Процес навчання нейронної мережі будемо розділяти на наступні етапи [1]:

— етап вихідного навчання;

— етап поточного навчання;

— відновлюваний етап навчання.

Вихідний етап навчання відповідає ситуації, коли користувач здійснює свою реєстрацію в мережі. Може скластися думка, що на етапі реєстрації досить ввести в систему ідентифікації дані, які надав користувач і ці дані використовувати для його ідентифікації. Практично виявляється, що в перебігу деякого початкового етапу роботи легального користувача в системі, його ідентифікаційні дані можуть змінюватися. Такі зміни не стосуються документальних даних, таких як пароль, ключ або інший засіб ідентифікації, яке визначається як незмінне в рамках системи захисту доступу. Для розвинених їх інформаційних систем, рівень безпеки яких обумовлюється комерційними факторами, для ідентифікації легальних користувачів мало використовувати тільки документальні засоби ідентифікації, тому, в таких системах використовуються профілі користувачів або формуються сигнатури користувачів. Такі структури або компоненти, в значній

мірі, наповнюються даними про користувачів на основі процедур навчання нейронної мережі. Нейронна мережа, в цьому випадку є базовим засобом для створення профілів або сигнатур користувачів. Оскільки формування профілів здійснюється на основі аналізу початкового становлення способів взаємодії користувача з інформаційною системою, то на цьому етапі і відбувається початкове навчання нейронної мережі. Таким чином, виникає перша проблема, яку необхідно вирішувати, це проблема визначення тривалості етапу вихідного навчання нейронної системи розпізнавання одного користувача.

У процесі використання послуг, які окремому користувачеві надає інформаційна система, може змінюватися, з боку користувача, потреба в кількості раніше зазначених послуг або потреба в тих чи інших параметрах відповідних послуг, більш того, якщо взяти до уваги, що користувач може являти собою групу окремих фахівців, які від імені однієї організації запитують ті чи інші послуги для вирішення загального завдання, то можливість зміни параметрів легального користувача не викликає сумніву. Очевидно, що система ідентифікації може вимагати, при кожній зміні параметрів окремого користувача, надання останнього офіційного підтвердження таких змін. Такий підхід до вирішення проблеми зміни параметрів ідентифікацій легального користувача, в ринкових умовах надання інформаційних послуг, є неприйнятним. Таким чином, виникає наступна проблема, яка полягає у визначенні моменту початку етапу поточного навчання та визначення тривалості цього етапу.

Вирішення цієї проблеми тісно пов'язане з проблемою розпізнання необхідності ініціації етапу поточного навчання, що дозволить гарантувати, що поточний етап навчання не виник у зв'язку з появою замаскованого нелегального користувача. Більш того, методи визначення необхідності ініціації поточного періоду навчання кошти ідентифікації, повинні розпізнавати будь-які можливі атаки, які можуть ініціюватися існуючими небезпеками, які існують по відношенню до інформації, що захищається інформаційною системою.

Відновлюваний етап навчання реалізується в тому випадку, коли з ініціативи легального користувача відбувається ініціалізація процесу навчання нейронної

мережі, для відтворення нового профілю легального користувача або підтвердження модифікованого профілю. Відновлювальний етап навчання може ініціюватися і без ініціації його легальним користувачем. Він ініціюється в тому випадку, якщо компоненти профілю, які являють собою паспортні дані, або дані, зміна яких регламентовано, виявляються порушеними. До паспортних даних відносяться паролі ключі та інші засоби, які можуть використовуватися як засоби з фіксованими значеннями.

Наведена класифікація етапів навчання нейронної мережі, яка використовується для побудови систем доступу, носить функціональний характер і відображає можливі періоди реалізації процесів навчання, які за своїм характером можуть бути різними з точки зору способу реалізації відповідного процесу. Можна виділити і інші типи етапів і відповідно інші способи реалізації процесів навчання. Ця можливість визначається способом інтерпретації процесів, які можуть відбуватися в системі доступу. Прикладом можуть служити етапи навчання, які визначені подіями, що відбуваються в системі доступу, наприклад, подіями, які визначаються виникненням атак на систему або події, пов'язані з виконанням системних перетворень або системного аналізу системи доступу та ін.

У зв'язку з цим, розглянемо основні методи навчання мереж, а так само розглянемо їх взаємозв'язок з особливостями використання нейронних мереж для формування систем захисту доступу. До основних методів реалізації навчання можна віднести наступні [1]:

— навчання з вчителем;

— навчання без вчителя;

— адаптаційне навчання.

Навчання з учителем полягає в наступному. На вхід мережі подається елемент навчальної вибірки $X = (x_1, ..., x_n)$, де n - кількість входів мережі. Саму мережу позначимо символом W. На виході мережі отримаємо вийшла вибірку $Y = (y_1, ..., y_m)$, де m - кількість виходів. Тоді навчання з учителем можна записати у вигляді наступного співвідношення:

$$S_i(W) = W\,[X_i,\, f\,(y_i, d_i)],$$

де $S_i(W)$ - стан мережі W на кроці навчання i, i - вхідні дані, де $x_i = (x_{i1}, ..., x_{in})$, y_i вихідні дані, які визначені як $y_i = (y_{i1}, ..., y_{im})$, d_i - еталонні дані, які відповідають кроку i, рівні $d_i = (d_{i1}, ..., d_{im})$. Дані d_i, це опис тих данних, котрі повинні вийти у випадку повністю навченої мережі, при подачі вхідних даних x_i. Це означає, що в ідеальному випадку, при повністю навченої мережі, повинно мати місце співвідношення $(y_i = d_i)$. Функція f описує спосіб визначення відповідності між y_i та d_i і, фактично, формує вхідний вектор таких даних, які по зворотним зв'язкам передається мережа з метою забезпечення наведеної рівності між y_i та d_i. Звичайно, що така ідеальна ситуація не може бути досягнута, оскільки, в цьому випадку, мережа перетвориться в детермінований перетворювач. Тому на основі співвідношення $\delta_i = \varphi\,(y_i, d_i)$ визначається величина міри навченості мережі або величина помилки роботи мережі, яка визначається за співвідношенням між y_i та d_i. У найпростішому випадку, функція $\varphi_i(y_i, d_i)$ може являти собою звичайну функцію порівняння. З урахуванням цього співвідношення, рівняння для стану мережі можна записати у вигляді наступного співвідношення:

$$S_i(W) = W\,[x_i,\, f\,(y_i, d_i)] + \varphi\,(y_i, d_i).$$

Що стосується функції $f\,(y_i, d_i)$, то, в найпростішому випадку, організації мережі W може являти собою різницю між елементами вихідних даних y_{ij} та відповідними елементами d_{ij}, але таке спрощення f не обов'язково.

У разі навчання без учителя, формально, стан мережі на поточному кроці навчання описується наступним співвідношенням:

$$S_i(W) = W\,(x_i, y_i).$$

В цьому випадку, використовується зворотний зв'язок для формування необхідного стану мережі $S_i(W)$. Процес навчання з використанням зворотного зв'язку називається навчанням з адаптацією. У разі навчання без адаптації, співвідношення для $S_i(W)$ запишеться у вигляді тривіальної рівності:

$$S_i(W) = W_i(X_i).$$

Вочевидь, що однокрокове навчання не використовується, оскільки воно може бути інтерпретовано, як інсталяція нейронної мережі. Навчання є процесом, який складається з ряду кроків. Тому, процес навчання описується у вигляді:

$$S_1(W) \to S_2(W) \to ... \to [S_m(W) = S_0(W)],$$

де $S_0(W)$ - стан навченої мережі.

У теорії навчання мереж [5] досліджуються, в першу чергу, методи модифікації елементів мережі на основі використання навчальної вибірки $\{x_1, ..., x_m\}$. Для реалізації таких змін, в першу чергу, вага вузлів мережі, використовується ряд правил, до яких відносяться наступні:

- правило Хебба;
- правило персептрона;
- правило дельта;
- правило Відрова-Хоффа;
- кореляційне правило;
- правило, відповідно з яким виграючий забирає все;
- правило вихідної зірки і ін.

Перш, ніж перейти до аналізу особливостей окремих правил, зупинимося на деяких загальних уявленнях про навчання мережі. Одним із загальних правил навчання мережі є наступне правило. Вектор вагів $\omega_i = [\omega_{i1}, ..., \omega_{in}]^t$ зростає пропорційно до кількості вхідних сигналів x_i і сигналів навчання γ_i. У загальному випадку цей сигнал можна описати у вигляді співвідношення

$$\gamma_i = \Psi\ (\omega_i, x_i, d_i).$$

Відповідно до загального правила навчання можна записати співвідношення:

$$\Delta\omega_i(t) = Cr\,[\omega_i(t), X(t), d_i(t)]\,x(t), \tag{3.1}$$

де Cr – постійна навчання, яка характеризує швидкість навчання. Для зручності, індексація кроків навчання записується зверху. В цьому випадку, можна записати наступне співвідношення:

$$W_i^{k+1} = W_i^k + C\gamma\,(W_i^k, X^k, d_i^k)\,X^k.$$

Правило Хебба використовується в ситуаціях, коли навчання проводиться без вчителя і записується у вигляді наступного співвідношення:

$$\Delta\omega_i = Cy_i x = Cf\,(W_i^t, x)\,x.$$

Фактично, це правило відповідає уявленням про зміни в аксонах з мікробіології. Правило персептрона використовується при навчанні з учителем. Навчальний сигнал являє собою різницю між відповіддю нейронної мережі, який мав би бути чи еталонний зразок відповіді і дійсним відповіддю, який отриманий від нейронної мережі, що записується у вигляді:

$$\gamma = d_i - y_i.$$

В цьому випадку, корекція ваги здійснюється відповідно до співвідношення:

$$\Delta\omega_i = C\,[d_i - \mathrm{sgn}\,(\omega_i^t x)]\,x.$$

Це правило відноситься до дискретних нейронних мереж, з функцією активації біполярного типу. Це означає, що коригування ваги відбувається тільки тоді, коли перетворення, яке здійснює нейрон є помилковим.

Правило дельта використовується для безперервних функцій активації для навчання за участю вчителя. Сигнал навчання формується відповідно до співвідношення:

$$r = \delta = [d_i - f\,(\omega_i^t x)]\,f'(\omega_i^t x),$$

де $f'(\omega_i^t, x)$ - похідна функції активації. Співвідношення для корекції ваги запишеться у вигляді:

$$\delta\omega_i = C\,(d_i - y_i)\,f'(net_i)\,x,$$

де $f'(net_i)$ - функція яка використовується для активації, наприклад $f'(net_i) = (1/2)(1 - y^2),\ C$ – арбітральная константа.

Правило Віндрова-Хоффа стосується навчання з вчителем, в разі використання довільної функції активації, в якому реалізується мінімізація середньої квадратичної помилки. Сигнал навчання визначається співвідношенням:

$$r = d_i - \omega_i^t x,$$

Корекція вектора ваги здійснюється у відповідності з наступним співвідношенням:

$$\Delta\omega_i = C\,(d_i - \omega_i^t x)\,x.$$

Кореляційне правило відповідає випадку, коли в загальному правилі навчання (3.1) приймається, що $r = d_i$. При цьому, корекція вектора ваги здійснюється відповідно до співвідношення:

$$\Delta\omega_i = Cd_i x.$$

Цей метод навчання найбільш доцільно використовувати при реалізації процесів запам'ятовування в мережі бінарної інформації.

Правило «який виграв забирає все» є прикладом правила з змаганням, яке використовується, як правило, для пізнання особливостей або властивостей на основі статистичних властивостей сигналів. Це правило використовується для процесів навчання без вчителя. Наприклад, якщо використовується однорівнева мережа, яка складається з P нейронів. Один з цих нейронів, наприклад, нейрон m формує найбільш сильну реакцію на вхідний сигнал. Такий нейрон являє собою виграваючим і єдиним, вага якого модифікується на поточному кроці навчання. Корекція вектора ваги здійснюється у відповідності з наступним співвідношенням:

$$\Delta\omega_m = \alpha\,(x - \omega_m),$$

де $\alpha > 0$ - коефіцієнт, який, як правило, зменшується в процесі проведення навчання. При цьому номер виграючого нейрона m визначається по співвідношенню:

$$\omega_{in}^t x = \max\,(\omega_i^t x).$$

Правило вихідної зірки використовується при навчанні з вчителем, але, при цьому, мережа визначає статистичні властивості вхідних і вихідних сигналів. Корекція ваги визначається відповідно до співвідношення:

$$\Delta\omega_i = \beta\,(d - \omega_i).$$

Коефіцієнт β являє собою невелике позитивне число, яке формується в процесі реалізації навчальної послідовності.

Нейронні мережі класифікуються згідно з такими ознаками [6]:

— за принципом побудови мережі або її архітектурі, яка визначається типом використаних зворотних зв'язків, типом використаних функцій активації, кількістю рівнів нейронних елементів та іншими структурними ознаками;

— за способом реалізації процесу навчання, який залежить від використаних правил навчання;

— по функціональної орієнтації нейронної мережі, яка визначається типом завдань, що вирішуються відповідною мережею.

Наведені ознаки є узагальненими і пов'язані між собою. Особливо, цей зв'язок проявляється між другою і третьою ознакою. Це підкреслює той факт, що нейронна мережа, як така, є об'єктом динамічним, оскільки тільки в процесі навчання і в процесі функціонування нейронна мережа проявляє свої властивості як окремий клас систем. Правила навчання, які наведені вище, можна застосовувати в різних комбінаціях і на різних етапах експлуатації мережі, що призводить до створення мережі з досить широкими функціональними можливостями.

3.2. Методи реалізації процесу навчання нейронних мереж для вирішення задач формування профілів користувачів

Залежно від завдань, які необхідно вирішувати за допомогою нейронних мереж, можуть вибиратися різні методи навчання нейронної мережі. Якщо використовувати нейронні мережі, для вирішення ряду завдань, наприклад, задач розпізнавання користувача, завдань виявлення атак на систему управління доступом, завдань протидії атакам і інших завдань, то методи навчання таких мереж будуть являти собою синтез різних алгоритмів навчання. Розглянемо основні концепції організації процесів навчання. Процес навчання нейронної мережі це такий процес, який призводить до зміни ваги нейронів, з яких складається мережа.

Одна з концепцій процесів навчання ґрунтується на уявленнях параметричного і непараметричного методів навчання. У разі параметричного методу, в процесі навчання змінюється величина ваги нейронів на основі оцінки параметрів, які характеризують об'єкти, з якими повинна працювати мережа. У разі непараметричних методів навчання, ваги нейронів змінюються безпосередньо в процесі навчання. В теорії нейронних мереж випадок, коли мережа повинна розрізняти два класи об'єктів, називається діхотомізатором. Розглянемо організацію процесу навчання діхотомізатора. Для цього, необхідно визначити величину коефіцієнта розподілу *C*. Оскільки діхотомізатори здійснюють розподіл вхідної інформації на два класи, коефіцієнт вибирається таким чином, щоб новий вектор ω^{k+1} на поточному кроці навчання виявився на гіперплощині, яка визначає клас вхідних даних поданих на вхід на кроці X^K. Тому, можна записати, що коефіцієнт *C* визначається відповідно до наступним співвідношенням:

$$C = (\left|\omega^{Kt} X^K\right|) / (\left\|X^K\right\|^2).$$

Одним з базових методів навчання є метод зворотнього проходження помилки. У цьому випадку алгоритм навчання модифікує вагу нейронів,

починаючи від виходу, на якому отримана помилка в напрямку входу, таким чином, щоб зміна ваги призвело до ліквідації помилки. Така помилка визначається на основі порівняння еталонного результату перетворення з реальним результатом, який отриманий, при проходженні X^K через нейронну мережу. Принциповою проблемою в цьому випадку є виникнення в функції помилки локальних мінімумів, оскільки порівняння може здійснюватися за допомогою довільної функції. У зв'язку з цим, виникає необхідність вирішення завдання збіжності процесу навчання. Найпростіший спосіб, що дозволяє уникнути затримку в локальних мінімумах, полягає в ініціації збільшення ваги на підставі еталонних вхідних даних, які подаються в довільній послідовності. Існує цілий ряд інших способів забезпечення збіжності процесу навчання, які ґрунтуються на відомих методах оптимізації функцій, якими описуються функції активації нейронів.

В силу своїх структурних особливостей, радіальні мережі відносяться до того класу мереж, які доцільно використовували для моделювання систем доступу. Тому, необхідно розглянути базові способи реалізації процесів навчання. Структура радіальних мереж передбачає існування в мережі центрів та базових функцій, які описують нейрони прихованих рівнів. Тому в процесі навчання необхідно реалізувати процедури вибору центрів, реалізувати процедури вибору параметрів базових функцій і, відповідно, здійснити процедури вибору ваги нейронів, які знаходяться на вихідному рівні. Вибір центрів, які відображають факт виділення кластерів, даних або образів, як це прийнято називати в теорії нейронних мереж [7], здійснюється наступними базовими методами:

— на підставі випадкового вибору;
— на підставі використання самоорганізації;
— на підставі навчання з вчителем.

У першому методі вибір центрів є найбільш простим. У цьому випадку вибір базових функцій виконується випадковим чином з використанням рівномірного розподілу. При виборі Функція Гауса розподілу, яка записується у вигляді:

$$G\left(\left\|X-t_i\right\|^2\right)=\exp\ \left(-\left(\left\|X-t_i\right\|^2\right)\right)\Big/\left(d^2/K\right),$$

де d - максимальна відстань між центрами t_i.

У разі використання самоорганізації, процес розподілу навчальних даних на кластери може бути представлений алгоритмом K- усереднений. При використанні сукупності векторів навчання X_2, кожен з них співвідноситься з відповідним центром. При цьому сукупність векторів приписаних до одного центру, утворює кластер, для якого новим центром є середнє поточних векторів, що описується співвідношенням:

$$t_i(K+1)=\left(1\big/N_i\right)\sum_{j=1}^{N_i}X_j(K),$$

де N_i означає кількість векторів $X_j(K)$, які приписані в k- тому циклі навчання до i-тому центрі. Визначення значень всіх центрів здійснюється паралельно.

Іншим підходом є використання ваговій міри відстані певного центру від поданого вектора X. Важливим є, в цьому випадку, вибір коефіцієнта навчання, який для радіальних мереж будемо позначати символом η. Адаптаційний метод вибору η складається в його залежності від часу навчання і зменшується з кожною поточної ітерацією k. Одним з відомих способів вибору η, при такому підході, є спосіб, який відповідає використанню співвідношення:

$$\eta\ (k)=\eta_0\ /(1+(k/T)),$$

де T- константа, яка представляє постійну часу. При $K<T$ величина η є постійною. При $K>T$ величина η зменшується експоненціально.

При використанні навчання, останнє можна будувати на основі зворотнього поширення. При цьому, функція мети описується у вигляді співвідношення:

$$E=(1/2)\sum_{j=1}^{P}\sum_{i=0}^{K}[W_i\varphi_i(X^{(j)}-d^{(j)})]^2.$$

У цьому випадку можна прийняти, що радіальна функція $\varphi_i(X)$ відповідає гаусівської функції:

$$\varphi_i(X)=\exp\ (-(1/2)[Q_i(X-t_i)]^T[Q_i(X-t_i),$$

де Q_i - матриця розміром $K \times K$.

Алгоритми навчання рекурентних мереж близькі до відповідних алгоритмів радіальних мереж. В обох випадках це градієнтні алгоритми мінімізації величин квадрата помилки між значеннями заданими на виході мережі $d_j(n)$ і значень, які реально отримані на виході мережі. Величина такої помилки описується співвідношенням:

$$E(n) = (1/2) \sum_{j=1}^{M} C_j^2(n),$$

де помилка визначається відповідно до співвідношення $C_j(n) = [d_j(n) - y_i(n)]$ для $j = 1, 2, ..., \gamma$ і $C_j(n) = 0$ в інших випадках. Використання градієнта обумовлюється тим, що метою навчання є вибір таких вагів, при яких мінімізується величина помилки, що формально записується у вигляді:

$$\nabla E_t = \frac{\partial E_t}{\partial W} = \sum_n \nabla E(n).$$

Рекурентне співвідношення, яке описує алгоритм Вільяма-Зінгера [8] і дозволяє швидко визначити похідну на поточному кроці, використовує похідну попереднього кроку:

$$\frac{\partial y_i(n+1)}{\partial W_{kl}(n)} = f'(u_i(n)) \left[\sum_{i \in B} W_{ji} \frac{\partial y_i(n)}{\partial W_{kl}(n)} + \delta_{kl} v_l(n) \right].$$

Цей алгоритм можна представити в такий спосіб.

1. Для кажного кроку n $(n = 0, 1, 2, ...,)$ необхідно скористатися співвідношеннями:

$$u_i(n) = \sum_{i \in (A \cup B)} W_{ij}(n)\, v_j(n),$$
$$y(n+1) = f(u_i(n)),$$

за допомогою яких, можна визначити стан всіх m нейронів. Завдяки цьому можна визначити вектор $v(n)$, який є активуючим для нейронів на момент n.

Вихідні значення вагів, які формують матрицю W формуються випадковим чином, використовуючи рівномірний розподіл.

2. За допомогою співвідношення.

$$R_{kl}^{j}(n+1) = f'(u_j(n))[\sum_{i\in B} W_{ij}\ (n)\ R_{kl}^{j}(n) + \delta_{kl} v_l(n)],$$

за умови, що початкове значення $R_{kl}^{j}(0) = 0$ необхідно визначити значення $R_{kl}^{j}(n)$ для відповідних індексів k, l, j, де $R_{kl}^{j}(n) = \partial y_i(n) / \partial W_{kl}(n)$.

3. Визначення поточних вагів здійснюється відповідно до залежності:

$$W_{kl}(n+1) = W_{kl}(n) + \eta \sum_{j=1}^{M} e_j(n)\ R_{kl}^{j}(n).$$

4. Кроки від 1 до 3 повторюються для наступних кроків.

Процес навчання нейронної мережі, фактично, являє собою процес формування у мережі таких характеристик, які забезпечували б можливість вирішення завдань, які характерні для систем управління доступом. Тому, розглянемо типи таких задач і обгрунтуємо вибір необхідних способів навчання нейронної мережі, яку приймемо в якості базового засобу для моделювання системи доступу. До згаданих вище завдань віднесемо наступні:

— формування стаціонарних образів користувачів;

— формування профілю користувача;

— розпізнавання та ідентифікація запиту на обслуговування, який сформував користувач;

— ідентифікація атаки на систему доступу;

— формування стратегії захисту локальної мережі або об'єкта, по відношенню до якого здійснюється управління доступом відповідною системою;

— реалізація протидії атакам;

— захист системи управління доступом.

Стаціонарні образи користувачів це сукупність тих даних, які використовуються для ідентифікації користувача, за умови, що користувач, який звертається за послугою, є легальним. Прикладом таких даних можуть служити

паролі, ідентифікатор, коди доступу та інші атрибути, які можуть використовуватися для ідентифікації і аутентифікації. Крім цих даних, до даних стаціонарного способу належать усі дані, які представляють собою легальну інформацію щодо легального користувача. Очевидно, що для реалізації в системі управління доступом стаціонарних образів легальних користувачів немає необхідності використовувати системи, які формуються на основі нейронних мереж. Нейронні мережі являють собою інструмент, який потрібен для перетворення інформації, яка надходить на вхід такої системи, якщо визначена мета такого перетворення. Випадок, коли нейронна мережа використовується для реалізації асоціативної пам'яті, що не суперечить такому визначенню функціональної орієнтації нейронної мережі, оскільки, асоціативна пам'ять побудована на основі розпізнання за вхідними даними інформації, яку необхідно прочитати з пам'яті, тому такий процес пов'язаний з розпізнаванням відповідних вхідних даних. Завдання розпізнання образів є типовими для задач, на вирішення яких орієнтовані нейронні мережі. Стаціонарний образ користувачів не може містити інформацію, яка змінюється в процесі використання користувачем послуги. Цей образ також не може змінюватися, минаючи прийняті протоколи обміну даними між користувачем і адміністратором мережі, незалежно від того перекладена ця функція на системне програмне забезпечення чи ні.

Профіль користувача, в загальному випадку, являє собою інформацію, яка описує всі або найбільш значущі особливості роботи легальних користувачів в середовищі, послугами якої відповідний користувач користується. Інформація, яка формує профіль, не може бути отримана стандартизованим способом так, як це реалізується при отриманні даних для стаціонарного образу. Прикладом даних, які відносяться до профілю користувача, можуть служити: характер що вирішують завдання, особливості обігу за ресурсами, які можуть інтерпретувати як почерк користувача, переважний час використання ресурсів мережі і цілий ряд інших особливостей, які відображають індивідуальні риси окремого користувача. Для формування профілю користувача вирішуються наступні завдання [9]:

— завдання класифікації образів;

— завдання розпізнання особливостей роботи з ресурсами мережі або системи, яка надає послуги користувачеві;

— завдання уточнення і розширення профілю користувача.

Завдання класифікації образів є типовою задачею, яка вирішується на основі використання нейронних мереж.

Завдання класифікації образів є типовою задачею, на вирішення яких орієнтовані нейронні мережі типу персептрона [6]. Під класифікацією або розпізнаванням мається на увазі ідентифікація вхідного образу і приписування його до певного класу. Класифікація образу здійснюється на основі реалізації окремих етапів початкового перетворення вхідних сигналів. Якщо використовувати сигнатури неприпустимої поведінки користувача, тоді можна говорити про розпізнавання нелегального користувача, що, по суті, є прямим завданням захисту мережі від несанкціонованого використання відповідних ресурсів. У разі досліджуваного підходу вирішується завдання визначення міри відхилення профілю користувача від його зразка, який на поточний момент сформований в системі управління доступом. Такий підхід до вирішення завдання захисту мережі від несанкціонованого доступу є більш гнучким у силу наступних обставин. Використання поточного профілю користувача для виявлення несанкціонованого доступу вимагає порівняння параметрів, які описують поточне звернення користувача до мережі, може бути неефективним в силу того, що почерк користувача може, до певної міри, від сеансу до сеансу варіюватися, що є допустимим. Використання тільки сигнатур, для розпізнання несанкціонованого доступу, може виявитися недостатнім, оскільки небезпека, яка може ініціювати атаки несанкціонованого доступу, формує їх таким чином, щоб розпізнати їх було не можливо. Тому сигнатури, як образи, можуть використовуватися тільки для розпізнання відомих атак. Очевидно, що цього не достатньо, тому, для розпізнавання атак необхідно використовувати рекурентні структури мереж з керованим кроком.

Розпізнавання та ідентифікація запиту користувача, по суті, є завданням контролю правильності роботи системи доступу, оскільки в даному випадку мова

йде не про захист системи від навмисних спроб несанкціонованого доступу, а про виключення помилкових ситуацій, які можуть виникати через випадкових звертань до мережі або помилок користувача. Може скластися враження, що такий контроль досить реалізовувати в рамках стаціонарних образів користувачів. Насправді, ситуація є більш складною. Справа в тому, що стаціонарна частина образу користувача містить мінімальну кількість даних про користувача, як правило, це ідентифікатор і пароль. Розширення атрибутів стаціонарної частини образу користувача не доцільне в зв'язку з тим, що їх збільшення істотно подовжує час доступу до системи, що є однією з ключових характеристик системи доступу. Тому, процес ідентифікації користувача ділиться на наступні етапи:

— ідентифікація користувача, для пропуску його в систему, яка надає послуги;

— ідентифікація користувача, що надає йому замовлені послуги;

— завершальна ідентифікація користувача.

При ідентифікації користувача, для пропуску його в систему, використовуються виключно паспортні, ідентифікаційні дані, для яких характерна їх обмежена кількість і наявність аутентифікованих компонентів. Під аутентифікованою компонентою мається на увазі компонента, яка є відомою в середовищі користувачів тільки одному користувачеві. Паспортні дані користувачів зберігаються в стаціонарному образі користувача. Після пропуску користувача в систему, вирішується завдання ідентифікації користувача по замовленим послугам і замовленим параметрам роботи користувача з системою. Серед параметрів, які використовуються для надання послуг, використовуються параметри, які відносяться і характеризують можливості самої системи. Наприклад, типи ресурсів, які надаються, час їх використання, інтенсивність надання ресурсів і інші. Оскільки, кожен з користувачів розглядається, як зовнішній агент, який незалежно від того використовує він в даний момент ресурси чи ні, є споживачем для даної системи, то параметри, що характеризують використовувані їм ресурси і режими його роботи з системою можуть змінюватися від запиту до запиту. Більш того, вони можуть змінюватися в межах

одного сеансу використання ресурсів мережі. Таким чином, значення параметрів ідентифікації, в результаті якої надаються ресурси мережі, не можуть бути постійними і, отже, вони повинні складати один з фрагментів профілю користувача. Користувач, крім типів і значень параметрів ресурсів, може характеризуватися ознаками, які специфічні для нього і характеризують виключно користувача. Прикладом таких параметрів можуть служити: переважний час роботи з системою, періодичність запитів на послуги, реакція на отримання послуги та інші індивідуальні властивості, які можуть ініціюватися виключно користувачем. Такі параметри складають окремий фрагмент профілю користувача, який на відміну від першого фрагмента, який називається системної частиною профілю (СПП), будемо називати персональної частиною профілю користувача (ППП). Завершальна ідентифікація користувача здійснюється в процесі повторення запитів користувача на надання послуг або ресурсів користувача. Необхідність введення таких різних видів ідентифікації обумовлюється наступними факторами:

- мінімізацією часу доступу до системи;
- підвищення рівня безпеки системи управління доступом;
- управління рівнем довіри до користувачів.

Мінімізація часу доступу до системи вимагає зменшення процедур перевірки окремого користувача, при його зверненні до системи. З іншого боку, підвищення рівня безпеки системи доступу вимагає збільшення кількості можливих перевірок користувача. Для вирішення цієї суперечності, кількість перевірок різних параметрів розбивається на окремі етапи ідентифікації, кожен з яких підвищує рівень довіри до користувача і в залежності від такого підвищення змінюється необхідність їх повторення в кожному окремому випадку звернення користувача до системи доступу. В рамках даного підходу існує можливість кількісного аналізу таких параметрів, як рівень довіри до користувача, необхідний час доступу для окремого користувача, кількість ідентифікуючих параметрів на різних рівнях ідентифікації і т.д.:

Ідентифікація атаки на систему доступу є окремою проблемою, хоча вона тісно пов'язана з завданням ідентифікації користувача. При вирішенні цієї проблеми, виникає ряд завдань, які вимагають окремого дослідження. До них належать такі завдання:

— визначення моменту або умов ініціації процесів ідентифікації атак;

— визначення рівня ефективності відповідної атаки;

— розпізнання небезпеки, яка ініціювала відповідну атаку;

— виявлення загроз, які використовуються розпізнаною атакою, для її реалізації.

Для вирішення перерахованих завдань в рамках системи управління доступом, необхідно виявляти інформацію, яка становить хоча б мінімум даних необхідних для вирішення перерахованих завдань. Природно припустити, що, в процесі вирішення цих завдань, інформація про атаки буде розширюватися. Основним засобом, за допомогою якого може накопичуватися і знаходиться відповідна інформація, є нейронна мережа, яка орієнтована на роботу з сигнатурами атак. Таким чином, сигнатури атак являють собою розвиваючу структуру даних про атаки.

3.3. Дослідження методів навчання нейронних мереж для вирішення задач протидії атакам на систему управління доступом

Завдання виявлення протидії атакам є прикладом завдань, методи вирішення яких і відповідно, алгоритми реалізації таких рішень, повинні постійно модифікуватися [10]. Така модифікація може відбуватися тільки на основі використання процесів навчання. Оскільки базовою середовищем, для реалізації систем доступу, є нейронні системи, то процеси навчання слід розглядати в рамках досліджень навчання нейронних систем [6].

Вихідними даними для вирішення завдань ідентифікації атак є сигнатури атак, які описують послідовності подій, що становлять реалізацію атаки.

Природно припустити, що використанню атак характерні наступні особливості [11]:

— атаки одного типу, які досить широко відомі, як правило, не вживаються, для реалізації несанкціонованого доступу в професійних цілях,

— нові атаки, як правило, формуються на основі модифікації відомих атак,

— модифікація та розширення програмних інструментальних засобів об'єктів атаки, є основними причинами, які визначають можливість появи нової атаки і можливість її успішної реалізації досягнення поставленої мети.

Розглянемо більш детально перераховані особливості і їх зв'язок з базовими засобами реалізації контролю доступу. В першу чергу приймемо, що система управління доступом, крім завдань управління, вирішує завдання захисту об'єкта, доступом до якому вона управляє. Таким чином, будемо вважати, що така система складається з підсистеми управління доступом і підсистеми захисту об'єкта, доступ до якого забезпечується підсистемою захисту, від атак типу несанкціонованого доступу. В даному випадку, будемо розглядати підсистему захисту від несанкціонованого доступу. Як уже підкреслювалося вище, однією з ЇЇ базових компонент є сигнатура атак. Сигнатура атак, в даному випадку, являє собою опис послідовності подій, які описуються в вигляді послідовності елементарних редукцій $x_i \to x_j$, де x_j - слідство, яке може мати інтерпретацію, що дозволяє говорити про можливе існування атаки або інтерпретацію, яка однозначно визначає факт атаки. У загальному вигляді, така послідовність може бути представлена наступним чином:

$$a_i = [(x_1 \to x_2)_1 \to (x_2 \to x_3)_2 \to ... \to (x_{n-1} \to x_n)_{(n-2)}] \qquad (3.2)$$

де x_n - має інтерпретацію атаки несанкціонованого доступу, якщо співвідношення (3.2) описує атаку. Звісно припустити, що в разі коли співвідношення (3.2) описує атаку, то починаючи з першої редукції, висновок x_2 вже можна інтерпретувати як подія, яка відповідає атаці. Така ситуація абсолютно не обов'язкова, оскільки будь-яка небезпека реалізує або яка ініціює атаку намагається формувати послідовність таким чином, щоб розпізнати її можна було тільки за останньою

редукції. Очевидно, що здатність системи управління доступом розпізнавати атаку на більш ранніх стадіях, кожна з яких може бути представлена номером редукцією, визначає міру рівня захищеності, яку забезпечує відповідна система доступу. Якщо прийняти, що одна послідовність подій описує процес реалізації атаки одного типу, то для опису атаки іншого типу використовується інша послідовність редукцій a_j. Інтерпретацію окремого події x_i будемо позначати $\Im(x_i)$. Всі основні інтерпретації подій x_i формуються при описі вихідних даних. Якби мала місце ситуація, в якій всі події x_i можна було б інтерпретувати як події відповідні процесу формування атак і події, які не відповідають цьому процесу, то рішення задачі розпізнання атак істотно спростилося б. Насправді, події, які можуть використовуватися для формування атаки, не можуть мати інтерпретації, яка однозначно відносила б відповідну подію до атаки. У зв'язку з цим виникає завдання визначення поточної події, яке в сукупності з існуючими його посилками може бути розпізнано як подія належать до атаки a_i. Виходячи зі співвідношення (3.2) можна наступним чином визначити факт існування успішної атаки, а також ввести інші визначення, які можуть використовуватися при аналізі і дослідженні атак. Розглянемо такі визначення.

Визначення 3.1 Атака a_i називається успішною, якщо вона розпізнана завдяки події x_n - яке є наслідком останньої редукції в співвідношенні (3.1).

Визначення 3.2 Рівень захищеності об'єкта, управління системою захисту визначається номером редукції r_i, наслідок в якій розпізнано як подія, відповідне реалізованої небезпекою атаки.

$$a_i = \{r_1 \to r_2 \to \ldots \to r_i \to \ldots \to r_n\}.$$

Визначення 3.3 Подія, яка допускає неоднозначну інтерпретацію і ділить в класифікації події на небезпечні і безпечні

$$\left[\left(x_i \to x_j\right) \to x_j \in a_i\right] \to \left[x_i \in \left(A \cup B\right)\right],$$

назвемо граничним. A - безліч подій належать атакам, B - безліч подій які не належать атакам.

Практика експлуатації обчислювальних мереж і систем така, що суворий поділ множин A і B неможливо. Тому, існує нетривіальне завдання розпізнання атак на обчислювальні мережі. Оскільки, в рамках системних засобів управління локальними мережами існує можливість реєстрації, практично, всіх подій, які відбуваються в мережі, то проблема розпізнання і виявлення атак зводиться до вирішення наступних завдань:

— виявлення послідовності подій або завдання формування з зареєстрованих подій окремих послідовностей;

— прогнозування розвитку послідовностей подій, які були розпізнані на поточний момент функціонування об'єкту захисту;

— визначення розпізнаних послідовностей, розвиток яких допускає можливість формування атаки.

Оскільки засоби захисту від атак, крім розпізнавання атак, як таких, ще й реалізують протидії певних подій і їх послідовностей, то в захищеній системі виникнення певних подій і, найчастіше, виникнення певних послідовностей подій, є неможливим. Тому систему захисту, орієнтовану на певний тип атак, будемо називати статичною системою захисту. Прикладом такого типу систем захисту може служити firewall [12]. Зазвичай статичні засоби захисту протидіють випадковим або непрофесійним спробам реалізації несанкціонованого доступу або спроб, пов'язаних з діями спрямованими на отримання інформації про стан рівня безпеки в різних фрагментах мережі. Тому розглядати ці типи захистів в даному випадку не будемо.

Будь-які події в мережі, крім послідовності їх виникнення, якщо така послідовність є відображенням залежностей між ними, характеризуються ще й інтервалами часу між окремими подіями. Тому, співвідношення (3.2) запишемо в наступному вигляді, який відповідає опису окремої атаки

$$a_i = \{(x_1 \to x_2) \to \tau_1 (x_2 \to x_3) \to \ldots \to \tau_{n-2} (x_{n-1} \to x_n)\}, \qquad (3.3)$$

де τ_i - інтервал часу між подією x_{i-1} і x_i в посилці $(x_{i-1} \to x_i)$. В даному випадку час між подіями x_1 і x_2 не береться до уваги, оскільки x_1, по суті, являє

собою псевдоподіями. Це означає, що x_1 являє собою причину ініціалізації відповідній послідовності посилок, яка може не бути сама по собі подією в тому сенсі, в якому йде мова про всі події в послідовності (3.2).

Співвідношення (3.2) може бути розширено не тільки до співвідношення (3.3). Справа в тому, що кожна поточне подія пов'язана з попереднім не тільки інтервалом часу, який між цими подіями виникає. Можна стверджувати, що для того, щоб після події відбулася подія x_j, необхідним є дотримання певних умов. В цьому випадку, співвідношення (3.3) може бути представлено у вигляді наступного співвідношення

$$a_i = \{(x_1 \to x_2) \to P_1\tau_1(x_2 \to x_3) \to \ldots \to P_{n-2}\tau_{n-2}(x_{n-1} \to x_n)\} \qquad (3.4)$$

де P_i - опис умов, які необхідно виконати для того, щоб подія, визначене редукцією $(x_i \to x_{i+1})$, могло бути виконано. Очевидно, що опис відповідних предикатів можна перенести всередину окремої редукції. Тоді кожна редукція може бути записана у вигляді

$$(P_i, x_i \to x_j).$$

Опис умов P_i будемо розглядати у вигляді предикатів, які такі умови будуть описувати у вигляді їх логічної апроксимації. Використовувати співвідношення (3.4) доцільно в разі, якщо попередня подія не забезпечує створення необхідних умов для ініціації виникнення наступної події. У більшості випадків, активні атаки проектуються таким чином, щоб поточну подію забезпечувало б виникнення всіх необхідних умов, для успішної ініціації наступних подій. У цьому випадку досить використовувати співвідношення (3.3). Використання різних τ_i при проектуванні атак характерно для тих випадків, коли атака в своїй основній частині складається в реалізації різних типів троянських коней або логічних бомб. Для цього типу програм характерним є існування одного ключового, тимчасового інтервалу τ_k, яким відповідна атака ділиться на дві базові частини:

— частина підготовки до реалізації атаки;

— частина реалізації активної атаки.

У цьому випадку співвідношення (3.3) можна представити в наступному вигляді:

$$a_i = \{(x_1 \to x_2) \to (x_2 \to x_3) \to \ldots \to \tau_k (x_i \to x_{i+1}) \to (x_{i+1} \to x_{i+2}) \to \ldots \to (x_{n-1} \to x_n)\}.$$

У зв'язку з викладеним описом атак, виникає задача визначення моменту ініціалізації процесів виявлення атаки. Звичайно припустити, що проблема визначення моменту ініціації процесу виявлення атаки тісно пов'язана з появою даних про те, що інформаційна система атакована певною небезпекою. Для вирішення цього завдання можна скористатися наступними підходами, кожний з яких використовує свої власні дані, отримані з інших джерел:

— підхід, який ґрунтується на аналізі статистичних даних про інтенсивності атак на даний об'єкт,

— підхід, який базується на рішенні задач прогнозування виникнення атак на об'єкт, що охороняється або локальну мережу,

— підхід, який базується на аналізі подій, які реєструються всередині мережі, яка охороняється відповідною системою управління доступом.

В даному випадку будемо досліджувати останній підхід до вирішення завдання визначення моменту ініціації процесу виявлення атак. З точки зору традиційних підходів до виявлення атак [13], ініціація процесів виявлення атак представляється доцільною, якщо атака по відношенню до об'єкту, що охороняється вже почалася. Такий підхід не дозволяє забезпечити достатньо високий рівень безпеки охоронюваної системи. Тому введемо наступні визначення.

Визначення 3.4 Небезпекою виникнення атаки по відношенню до захищаємого обьекту назвемо таку ситуацію, коли в системі захисту реєструються події, які не передбачені штатними умовами функціонування об'єкта охорони або мережі, яка захищається.

Формально, це визначення можна записати :

$$[(x_i \notin U_s) \& [(x_i \in a_i) \vee (x_i \notin a_i)]] \to (x_i \in \sigma),$$

де σ - безліч подій, які відносяться до подій, що визначає небезпеку виникнення атак. Як уже зазначалося, кожна атака, для своєї успішної реалізації використовує погрози, якими володіють об'єкти охорони і засоби захисту. Таким чином визначення 3.4 можна доповнити наступними додатковими умовами, які дозволяють більш детально описувати ознаки появи небезпеки атаки. До таких умов відносяться такі.

Умова 3.1 Кожна небезпечна подія ξ_i відбувається завдяки використанню конкретних загроз, які існують в об'єкті захисту.

Формально, це визначення можна записати:

$$[x_i(\eta_i) \& x_i \notin U_s] \to (x_i = \xi_i),$$

де η_i - загроза, яка існує в об'єкті або системі захисту відповідного об'єкта.

Насправді такі параметри об'єктів, як загрози в більшості випадків невідомі. Тому, одним із завдань системи захисту є виявлення відповідних загроз і визначення величини їх значень. Справа в тому, що наявність загрози не обов'язково визначає необхідність її ліквідації, оскільки це може спричинити за собою необхідність суттєвої переробки самого об'єкта. Тому, одним із завдань системи захисту, є завдання виявлення загроз, їх нейтралізація або зменшення їх значень.

Розглянемо наступні функції, які необхідно виконувати системі захисту в процесі її функціонування, яке може відбуватися незалежно від функціонування захищається системи:

— виявлення небезпеки виникнення атаки,

— визначення ефективності потенційної атаки,

— виявлення атак,

— виявлення загроз, які існують в системі,

— усунення або зменшення величини значення загроз, які виявлені в об'єкті, що захищає.

Розглянемо більш детально процеси виявлення небезпек ξ_i , які, як і загрози можуть виникати в системі. На відміну від атак a_i - які завжди ініціюються

зовнішніми небезпеками, внутрішні небезпеки, які для зручностей термінологічних, будемо називати критичними подіями в системі, виникають в результаті наступних причин, які обумовлюються різними факторами:

— проникненням атаки і початковими етапами її розвитку в системі,

— випадковими чинниками, які не пов'язані з ініціацією атаки зовнішньою небезпекою,

— змінами параметрів загроз, до яких призводять процеси легального функціонування захищаємої системи.

Співвідношення (3.4) може описувати не тільки атаку a_i але і будь-який процес, який з тих чи інших причин може зародитись в охоронній системі. Якщо в системі реєструються системними засобами все без винятку події, то причиною того, що можлива атака або деякий внутрішній фактор може виявитися не виявленим, будуть наступні обставини:

— якщо відповідне подія не ідентифікується як таке, що $x_i \notin U_s$, оскільки його параметри лежать в межах параметрів допустимих подій, але істотно впливає на процеси в системі,

— в силу великої кількості подій, які відбуваються в системі, небезпечна подія, що не має явно виражених ознак неприпустимої події, може бути пропущена, як подія незначна на момент його появи,

— якщо системні засоби мають можливість сепарувати події перед їх реєстрацією, то відповідна подія може виявитися взагалі незареєстрованим.

Беручи до уваги наведені вище обставини, можна сформулювати наступну задачу. На який редукції в співвідношенні (3.4) буде виявлена атака, при заданому рівні безпеки або заданому рівні захисту системи. Для вирішення цього завдання, необхідно визначитися з визначенням і способом обчислення рівня захищеності системи. Такий рівень забезпечується в рамках системи управління доступом, підсистемою захисту. Основою функціонування системи захисту є процеси виявлення атак і процеси протидії атакам. В основі виявлення атак лежить використання моделей загроз, які, за визначенням, є властивостями об'єкта, який

охороняється. Такі компоненти будемо позначати буквою m. Ці компоненти, крім вже визначених вище загроз η розширюються наступними елементами. Нехай деяка небезпека в процесі розвідки об'єкта виділила ряд загроз, які не відображені в підсистемі захисту (PSZ), , як характеристики об'єкта, що захищається. В цьому випадку, відповідна послідовність подій $x_1,\ldots,x_i,\ldots,x_m$, у співвідношенні з (3.4) та (3.3) повинна доповнюватися тимчасовими мітками τ і предикатами P_i, які описують умови, що змінюються або фактори середовища, безпосередньо пов'язані з відповідними подіями. Прикладом таких факторів можуть служити інтенсивність передачі даних через певний канал, обсяг використаної пам'яті на даному поточному інтервалі часу τ і т.п. Тому, кількість моделей загроз, які визначені в PSZ і представлені як моделі загроз, може визначати міру безпеки окремої системи. Таким чином, рівень захисту, який забезпечує система PSZ буде в кількісному вигляді визначатися співвідношенням:

$$W(U_s \cup U_N) = \sum_{i=1}^{m} \eta_i$$

У зв'язку з тим, що кількість погроз η може протягом часу функціонування системи змінюватися, тому $W(U_s)$ теж може змінюватися. У такому способі оцінки величини $W(U_s)$ не враховуються невідомі загрози, які можуть бути виявлені в процесі виявлення атак a_i. В цьому випадку, виявлення атак грунтується на аналізі предикатів P_i в співвідношенні (3.4). інтервали τ_i з (3.4) спільно з предикатами, дозволяють не тільки виявити атаку яка використовує невідому загрозу, а й сформувати її модель. Доведемо наступне твердження.

Твердження 3.1 Якщо в системі U_s виділена атака, то на основі аналіза атаки можно сформувати модель загрози, котра відповідною атакою була використана.

Формально це можна записати у вигляді:

$$\{[(x_1 \to x_2) \to \tau_1 P_1 (x_2 \to x_3) \to \ldots \to \tau_{n-2} P_{n-2} (x_{n-1} \to x_n)] \& (r_i \to a_i)\} \to m_i(\eta_i),$$

де r_i редукція на якій виявлена атака або в формальний запис $[\tau_i P_i (x_{i+1} \to x_{i+2})] = r_i; m_i(\eta_i)$ - модель загрози η_i. Відповідно до визначення, P_i описує поточну зміну в стані U_s, до якого привела редукція r_i. Модель $m_i(\eta_i)$ є опис тих

властивостей елементів U_s, які дозволяють реалізовувати редукцію $r_i = (x_{i+1} \to x_{i+2})$. Опис ситуацій в U_s може містити не тільки одне P_i, але і цілий ряд $P_i, P_{i+1}, \ldots, P_{i+k}$. Тому можна записати, що $m_i(\eta_i) = P_i \,\&\, P_{i+1} \,\&\, \ldots \,\&\, P_{i+k}$. Загроза η_i це така властивість або така ситуація в U_s, яка є неприпустимою, оскільки вона визначає можливість появи нештатних подій x_j, які визначають можливість виникнення позаштатних процесів $[(x_i \to x_{i+1}) \to \ldots \to (x_{i+k} \to \xi_j) \to \ldots]$. Тому ті ситуації $(P_i \,\&\, P_{i+1} \,\&\, \ldots \,\&\, P_{i+k}) \to \xi_j$ що визначають опис η_i, що можна представити у вигляді:

$$\{[(P_i \,\&\, P_{i+1} \,\&\, \ldots \,\&\, P_{i+k}) \to x_j] \,\&\, (x_j \notin U_s)\} \to [(P_i \,\&\, P_{i+1} \,\&\, \ldots \,\&\, P_{i+k}) m_i(\eta_i)].$$

Приймемо, що в результаті використання η_i, яка не входить в $(U_s \cup U_N)$ або $\eta_i \notin (U_s \cup U_N)$, виявлено r_i^k, де r_i^k - критична редукція. Це означає, що в послідовності $(x_1 \to x_2) \to \ldots \to \tau_{i-2} P_{i-2}(x_{i-1} \to x_i) \to \ldots \to \tau_{n-2} P_{n-2}(x_{n-1} \to x_n), r_i^k = (x_{i-1} \to x_i)$, а подія x_i розпізнано, як подія яке ідентифікується, як підозріле, або $x_i \in U_N$. Тоді можна сформувати протилежний ланцюжок фрагменту $[(x_1 \to x_2) \to \ldots \to \tau_{i-2} P_{i-2}(x_{i-1} \to x_i)]$, що формально описується співвідношенням $F[(x_1 \to x_2) \to \ldots \to \tau_{i-2} P_{i-2}(x_{i-1} \to x_i)] = [(x_i \to x_{i-1}) f_{i-2}(P_{i-2}) \tau_{i-2}^{-1} \to \ldots \to (x_2 \to x_1)] \to m_i(\eta_i)$, де $f_{i-2}(P_{i-2}) = (P_{i-2} \to P_{i-3})$.

Оскільки, для фрагмента $[P_{i-2}(x_{i-1} \to x_i) \to P_{i-1}(x_i \to x_{i+1})] \Rightarrow$ $\Rightarrow (P_{i-2} \to P_{i-1}) \,\&\, [(x_{i-1} \to x_i) \to (x_i \to x_{i+1})]$ то може бути побудовано таке перетворення F, яке поширеться на весь ланцюжок залежностей $(x_1 \to x_2) \to \ldots \to \tau_{i-2} P_{i-2}(x_{i-1} \to x_i) \to \ldots \to \tau_{n-2} P_{n-2}(x_{n-1} \to x_n)$, що і доводить твердження.

3.4. Дослідження методів самоорганізації нейронних систем для вирішення задач розпізнавання атак

При реалізації засобів захисту від атак, по відношенню до відомих атак існує можливість досить повно відгородитися від можливості успішного завершення такої атаки. У більшості випадків атаки, які робляться по відношенню до захищених об'єктів, є модифікаціями відомих атак або новими

атаками, які до теперішнього моменту не використовувалися. Тому найважливішими завданнями є:

— розпізнавання нових атак;

— прогнозування атак;

— ідентифікація атак.

Завдання ідентифікації атак, при використанні нейронних систем, для реалізації засобів захисту, вирішується досить легко, оскільки, в цьому випадку вона зводиться до розпізнання образу атаки по сигнатурі, яка відповідну атаку описує. В цьому випадку, ефективність розпізнання атак буде залежати від якості сигнатури.

Завдання розпізнання нових атак і завдання збільшення ефективності розпізнання атак використовує сигнатури атак вирішується на основі використання такої властивості нейронних мереж, як властивість її самоорганізації, яке є вищим за рівнем методів зміни можливостей мережі в порівнянні з методами навчання. Принциповою відмінністю методів навчання від методів самоорганізації є наступне. При навчанні накопичується інформація, яка вводиться в систему навчання. Завдяки навчанню, система володіє більш різноманітною інформацією, якщо остання повинна здійснювати ті чи інші дії, наприклад, ідентифікацію розпізнаючого образу. При навчанні відбувається накопичення даних, які вводяться в систему в процесі навчання. При цьому, дані, як окрема, незалежна частина об'єкта навчання, можуть в процесі навчання модифікувати свою структуру, за допомогою ускладнення організації структури даних. При цьому, сама система не зазнає ніяких змін.

У разі самоорганізації використовуються механізми, які призводять до змін в самій системі. Такі зміни стосуються найбільшою мірою тих компонентів, які реалізують такі процеси як прийняття або формування рішень, на які орієнтована система для вирішення завдань певного типу. Очевидно, що процеси самоорганізації також використовують різні способи навчання. Це означає, що при реалізації таких процесів в нейронну мережу вводяться нові дані, а також змінюються механізми аналізу цих даних. Таким чином, можна стверджувати, що

самоорганізація певних об'єктів являє собою процедуру введення нових знань. Процеси самоорганізації можуть ініціюватися зовнішніми факторами або внутрішніми факторами, які можуть мати місце у відповідній системі.

Самоорганізація нейронних мереж ініціюється в більшості випадків зовнішніми факторами і грунтується на використанні нової інформації, що вводиться. Розглянемо більш детально відомі механізми реалізації процесів самоорганізації в нейронних мережах різних типів і проаналізуємо особливості використання цих механізмів для вирішення завдань пов'язаних із захистом, які здійснюються системами управління доступу.

Серед відомих механізмів самоорганізації нейронних систем виділяється два базові підходи до їх реалізації в нейронних мережах різних типів [14]:

— механізми самоорганізації, які ґрунтуються на аналізі взаємозалежностей між сигналами в процесі навчання нейронної мережі;

— механізми самоорганізації, які ґрунтуються на аналізі взаємозалежностей між нейронами, які змінюються в процесі навчання.

У першому випадку використовуються правила Хебба, а в другому випадку використовуються узагальнене поняття про правила Кохонена. Процес самоорганізації другого типу грунтуються на явищі конкуренції між окремими нейронами під час процесів навчання. У цьому випадку мова йде про звичайні однорівневі мережі, в яких кожен нейрон пов'язаний з усіма складовими N-мірного вхідного вектора X. Ваги з'єднань семантичних нейронів формують вектор $w_i = [w_{i1}, ..., w_{iN}]^T$. При подачі на вхід нейронної мережі навчальної вектора X, за умови, що він нормалізований, нейрон переможець визначається співвідношенням:

$$d(X, w_w) = \min_{1 \le i \le n} d(X, w_i),$$

де $d(X, w)$ відстань між вектором X і вектором w, n- кількість нейронів. Відстань визначається в рамках обраної метрики. Нейрон переможець і все нейрони, що знаходяться в найближчій околиці від нейрона переможця

підлягають адаптації. Така адаптація полягає в зміні вектора ваги в напрямку значень вектора X, відповідно до правила [15]:

$$w_i(K+1) = w_i(K) + \eta_i(K)[X - w_i(K)],$$

де $i \in S_w(K)$ - номера нейронів з найближчого оточення нейрона переможця, $\eta_i(K)$ - коефіцієнт навчання i - того нейрона в момент навчання K. Величина $\eta(K)$, зменшується при збільшенні відстані між нейроном переможцем і нейронами з найближчого оточення зі збільшенням відстані між ними.

При реалізації такого підходу до вирішення завдання самоорганізації, принциповим є вибір метрики, в якій будуть вимірюватися відстані між векторами X і w_i. Найбільш поширеними метриками є:

— метрика евклідового простору:

$$d(X, w_i) = \|X - w_i\| = \sqrt{\sum_{j=1}^{N}(x_j - w_{ij})^2},$$

— метрика, яка визначається скалярним витвором двох векторів:

$$d(X, w_i) = (-X \cdot w_i = 1 - \|X\| \|w_i\| \cos(X, w_i),$$

— метрика, яка визначається нормою L_1

$$d(X, w_i) = \sqrt{\sum_{j=1}^{N}|x_j - w_{ij}|}.$$

Другою важливою проблемою є нормалізація вхідного вектора, який подається на вхід в процесі навчання. Нормалізація вхідного вектора може реалізуватися у відповідності з наступними способами [6]:

— шляхом перевизначення складових вектора відповідно до співвідношення:

$$\left[(x_i)/\left(\sqrt{\sum_{i=1}^{N} x_i^2}\right)\right] \to x_i;$$

— шляхом збільшення розмірності простору на одиницю, що реалізується з використанням співвідношення:

$$\sum_{i=1}^{N+1} x_i^2 = 1.$$

В теорії нейронних мереж використовується поняття про мертві нейрони. При випадковій ініціалізації ваги мережі, може скластися ситуація, коли частина

нейронів виявиться в області, для якої дані будуть відсутні або їх зміна буде незначна. В цьому випадку, вхідні дані будуть використовувати меншу кількість нейронів по відношенню до всіх нейронів мережі. Такі невживані нейрони будуть називатися мертвими нейронами. В цьому випадку виникає проблема активізації всіх нейронів. Вирішення цієї проблеми можливе в тому випадку, якщо в алгоритмі навчання враховувати кількість перемог поточних нейронів. В цьому випадку, нейрон, який виявився переможцем, після перемоги деякий інтервал часу залишається пасивним, що прийнято називати відпочинком, тобто нейрон після перемоги деякий час відпочиває. Такий підхід до вирішення цієї проблеми називається механізмом втоми. Реалізація такого механізму полягає у введенні поняття потенціалу P_i для кожного нейрона. В цьому випадку, при подачі на вхід нейронної мережі вектора навчання X_i, для модифікації вибирається нейрон, який задовольняє наступному співвідношенню між потенціалами нейрона:

$$\{[(i \neq w)\,\&\,(P_i(K+1))] \rightarrow [P_i(K+1) = P_i(K) + (1/n)]\}\,\&$$
$$\{[(i = w)\,\&\,(P_i(K+1))] \rightarrow [P_i(K+1) = P_i(K - P_{\min})]\},$$

де потенціал $P_{\min}$ визначає мінімальний потенціал, при якому можлива участь відповідного нейрона в змаганні на K-тому шазі навчання.

Величина потенціалу $P_{\min}$ визначається на інтервалі [0,1]. Якщо $P_{\min} = 0$, то не відбувається втоми нейронів і кожен з них приймається готовим до чергового змагання. При $P_{\min} = 1$, з'являється наступна крайність.

Алгоритм навчання, з урахуванням кількості перемог нейрона, при обчисленні відстані їх ваги від вхідного вектора X, реалізує модифікацію нейрона, яка прямо пропорційна кількості перемог, яке цей нейрон мав на минулих етапах навчання. Формально, це можна записати у вигляді:

$$N_i d\,(X, w_i) \rightarrow d\,(X, w_i).$$

Це співвідношення означає, що чим більше у нейрона було перемог, тим більше збільшується відстань $d\,(X, w_i)$ між вектором ваги і вхідним вектором навчання X.

Метою навчання самоорганізованих мереж на основі конкуренції між нейронами є такий підбір нейронів (підбір величини ваги нейронів), при якому мінімалізується величина спотворення, яке представляється як величина помилки, яка допускається, при апроксимації вхідного вектора X вагами нейронів. При вхідних векторах X і використанні евклідової норми, така помилка визначається співвідношенням:

$$E_q = (1/2)\sum_{i=1}^{P}\left\|x_i - w_{w(i)}\right\|^2,$$

де $w_{w(i)}$ - вага нейрона, який переміг під час подачі на вхід мережі вектора X_i.

Процес адаптації вектора ваги може бути описаний залежністю у вигляді:

$$\{w_i + \eta_i G(i, X)[X - w_i]\} \to w_i.$$

Це співвідношення справедливо для всіх нейронів i, які є найближчим оточенням нейрона переможця. Найбільш популярним алгоритмом навчання самоорганізуючої мережі на основі принципу конкуренції, є алгоритм, для якого функція для визначення сусідів записується у вигляді наступного співвідношення:

$$\{[(d(i, w) \le \lambda)\,\&\,G(i, X)] \to [G(i, X) = 1]\}\,\&$$
$$\&\,\{[(dL_i, w) > \lambda)\,\&\,G(i, X)] \to [G(i, X) = 0]\}.$$

Коефіцієнт λ є радіусом, який визначає сусідні нейрони, величина якого в процесі навчання прагне до нуля. Такий тип сусідства прийнято називати прямокутним сусідством.

Другий тип сусідства називається гаусовим сусідством і описується виразом:

$$G(i, X) = \exp[-(d^2(i, w))/2\lambda^2].$$

Важливим алгоритмом самоорганізації є алгоритм, який називається алгоритмом нейронного газу [16]. У цьому алгоритмі, після кожної ітерації всі нейрони сортуються залежно від їх відстані від вектора X, що записуються у вигляді:

$$d_0 < d_1 < d_2 < \ldots < d_{n-1}.$$

Значення функції сусідства для i-того нейрона описується співвідношенням:

$$G(i, X) = \exp(-(m(i))/\lambda),$$

де $m(i)$ - черговість нейронів, яка отримана в результаті сортування. Якщо параметр $\lambda = 0$, то адаптації піддається тільки нейрон переможець. Якщо $\lambda \neq 0$, то адаптації підлягає цілий ряд нейронів, для яких змінюється величина ваги відповідно до значення функції $G(i, X)$. Для досягнення гарних результатів самоорганізації, процес навчання повинен починатися при великих значеннях λ і на протягу часу навчання λ має зменшуватися. Таке зменшення λ може здійснюватися за лінійним законом, або за степеневим законом відповідно до співвідношення:

$$\lambda(K) = \lambda_{\max}(\lambda_{\min} / \lambda_{\max})^{K/K_{\max}},$$

де $K_{\max}$ - максимальну кількість ітерацій.

Якщо мова йде про обробку багатовимірних даних, то необхідно певним чином упорядкувати нейрони. Таке впорядкування полягає в тому, що дані з багатовимірного простору проектуються в двох або принаймні трьох мірний простір, зберігаючи при цьому базові властивості розподілу в багатовимірному просторі. Приймемо, що маємо n векторів в N-мірному просторі X_i. Відповідно до них визначається n векторів в M-мірному просторі $(M = 2,3)$, які позначаються як y_i. Нехай відстані між ними в N-мірному просторі описуються у вигляді $d_{ij}^* = d(X_i, X_j)$, у просторі M-мірному $d_{ij} = d(y_i, y_j)$. Нелінійне перетворення полягає в тому, щоб так підібрати вектори y, щоб мінімізувати функцію помилки, яка описується співвідношенням:

$$E = (1/C)\sum_{i<j}^{n}([d_{ij}^* - d_{ij}]^2)/d_{ij}^*,$$

де $C = \sum_{i<j}^{n} d_{ij}^*$, $d_{ij} = \sqrt{\sum_{K=1}^{M}[y_{iK} - y_{jK}]^2}$, де y_{ij} означає j-ту складову вектора y_i.

Коли для реалізації процесів самоорганізації використовуються взаємозалежності між сигналами, то такі процеси самоорганізації називаються кореляційними або Хеббовскімі. До такого типу мережі відносяться два типи мереж:

— мережу, яка виконує декомпозицію даних головних складових, або мережу типу PCA;

— мережу, яка виконує декомпозицію систему адаптації на незалежні складові, або мережу ICA.

Ці дві мережі за своєю природою є лінійними мережами. Базове правило Хебба пов'язано з лінійною моделлю нейрона, що описується співвідношенням:

$$y_j = \sum_{i=0}^{N} w_{ji} x_i.$$

Відповідно до постулатом Хебба, зміна ваги нейрона, після подання вектора X, описується наступним виразом:

$$\Delta w_{jK} = \eta\,(y_i - y_i^{(0)})(x_K - x_K^{(0)}),$$

де $y_i^{(0)}$ і $x_K^{(0)}$ - певні постійні, η - коефіцієнт навчання. З урахуванням, перед усім тим натовпом навчальних векторів, зміна ваги мережі в часі можна представити у вигляді наступного співвідношення:

$$\frac{dw_{jk}}{dt} = \sum_{i=1}^{N} w_{ji} C_{ik} + \frac{K_2}{N} \sum_{i=1}^{N} w_{ji} + K_1,$$

де K_1 і K_2 - певні постійні, які пов'язані з $x_K^{(0)}, y_j^{(0)}$ і η, C_{iK} - середня коваріація активності i - того і k -того нейронів, яка описується наступним співвідношенням:

$$C_{iK} = (1/P)\sum_{j=1}^{P} (x_i^{(j)} - x_i)(x_k^{(j)} - x_k),$$

де постійна x_i означає усереднене значення еталонів вхідних, яка відповідає i -тої складової усередненого вектора $\overline{X}$, де $X = (1/P)\sum_{K=1}^{P} x^{(K)}$.

Якщо зміна ваги здійснюється відповідно до правила найбільшого спуску енергетичної функції *E*, то отримаємо:

$$\frac{dE}{dw_{jk}} = -\frac{dw_{jk}}{dt} = -\sum_{i=1}^{N} w_{ji} C_{ik} - K_1 - (K_2/N)\sum_{i=1}^{N} w_{ji}.$$

Вирішуючи це диференціальне рівняння, отримуємо енергетичну функцію у вигляді [4]:

$$E = E_v + E_K;$$

де

$$E_v = (-1/2)\sum_{i=1}^{N}\sum_{K=1}^{N} w_{ji} C_{ik} w_{kj}$$
$$E_K = -K_1 \sum_{i=1}^{N} w_{ji} - (K_2/2N)\left(\sum_{i=1}^{N} w_{ji}\right)^2.$$

Перша складова енергетичної складової E_v визначає варіацію σ_j^2 активності j-того нейрона. Друга складова може бути ототожнена з складової штрафу енергетичної функції.

Нехай $X = [x_1, x_2, ..., x_N]^T$ є імовірнісним вектором з нульовим середнім значенням. Нехай $R_{XX} = E[XX^T] = \langle XX^T \rangle$ означає значення автокореляційної матриці, по всіх векторах X. Цю матрицю можна записати у вигляді:

$$R_{XX} \approx (1/P)\sum_{K=1}^{P} X_K X_K^T = (1/2)\, XX^T,$$

де матриця даних X формує поточний вектор навчання $X = [x_1, x_2, ..., x_P]$. Позначимо через λ_i власне значення матриці автокореляції R_{XX}, а через w_i ортогональні вектори власних значень, асоційованих з ними. Власні значення і власні вектори пов'язані між собою залежністю:

$$R_{XX} w_i = \lambda_i w_i,$$

де $i = 1, 2, 3, ..., N$. Матриця W перетворення декомпозиції по головних складових визначається у вигляді $W = [w_1, w_2, ..., w_K]^T$. В цьому випадку перетворення запишеться у вигляді:

$$y = W_X.$$

Вектор $y = [y_1, y_2, ..., y_K]^T$ являє собою вектор головних складових, які мають найбільший вплив на реконструкцію вектора даних $X = [x_1, x_2, ..., x_N]^T$. З точки зору статистики, перетворення визначає безліч K ортогональних векторів, які вносять найбільший вклад в варіацію вхідних даних. Реконструкція X на основі вектора y і ортогональної матриці W відбувається відповідно до залежності:

$$\hat{X} = W^T y.$$

Подання вектора даних X за допомогою найбільших головних компонентів $y_1, y_2, ..., y_K$, що формують вектор y і відповідає збереженню інформації про максимальну порцію енергії, яка міститься в множині даних.

Для визначення першої головної компоненти y_1 і пов'язаного з нею вектора w_1, який відповідає матриці R_{XX}, використовується система з одного лінійного нейрона, який описується співвідношенням:

$$y_1 = w_1^T X = \sum_{j=0}^{N} w_{1j} x_j.$$

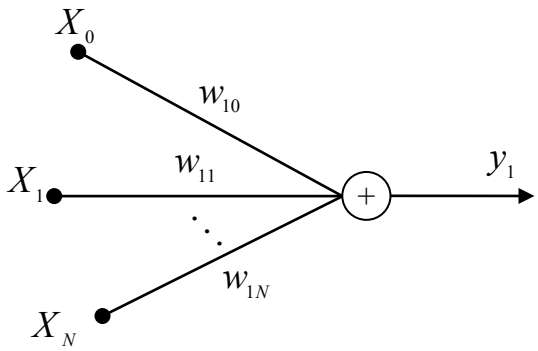


Рисунок 3.4.1 – Нейронна мережа для визначення однієї головної складової

На рисунку 3.4.1 приведена схема такого нейрона. Підбір ваги вектора w_1 реалізується відповідно до нормалізованими правилами Хебба, які формально описуються наступним чином:

$$w_{1j}(K+1) = w_{1j}(K) + \eta y_1(k)[X_j(k) - w_{1j}(k)\, y_1(k)],$$

де $\eta(k)$ - коефіцієнт навчання. Перша складова відповідає звичайному правилу Хебба, а друга складова реалізує самоорганізацію вагових векторів.

Для визначення наступних складових відповідного перетворення, необхідно використовувати більше нейронів у вхідному шарі. Кількість нейронів відповідає кількості складових. У цьому випадку більш ефективним є правило Сангера [9], для якого вхідні сигнали генеруються відповідно до співвідношення:

$$y_i(k) = \sum_{i=0}^{N} w_{ij}(k)\, x_j(k).$$

Адаптація ваги нейронної мережі здійснюється у відповідності з наступним співвідношенням:

$$w_{ij}(K+1) = w_{ij}(k) + \eta y_i(k)[x_j(K) - \sum_{h=1}^{i} w_{hj}(k)\, y_h(k)].$$

Розглянемо алгоритми самоорганізації, що виконують декомпозицію систему адаптації на незалежні складові або алгоритми ICA. Один із способів реалізації

такого алгоритму ґрунтується на розділенні сигналів $S_i(t)$ на основі інформації, яка знаходиться в їх лінійній суперпозиції. Нехай маємо n незалежних сигналів $S_i(t)$ та відповідну матрицю A

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}.$$

Приймемо, що для вимірювання доступний єдиний сигнал $x_i(t)$, який є лінійною суперпозицією $S_i(t)$, що описується співвідношенням:

$$x_i(t) = \sum_{j=1}^{n} a_{ij} S_i(t).$$

При цьому a_{ij} і $S_j(t)$ - невідомі. Якщо прийняти, що сигнали статично незалежні, то для вирішення проблеми можна використовувати нейронну мережу. При цьому схема підключення нейронної мережі приведена на рис. 3.4.2.

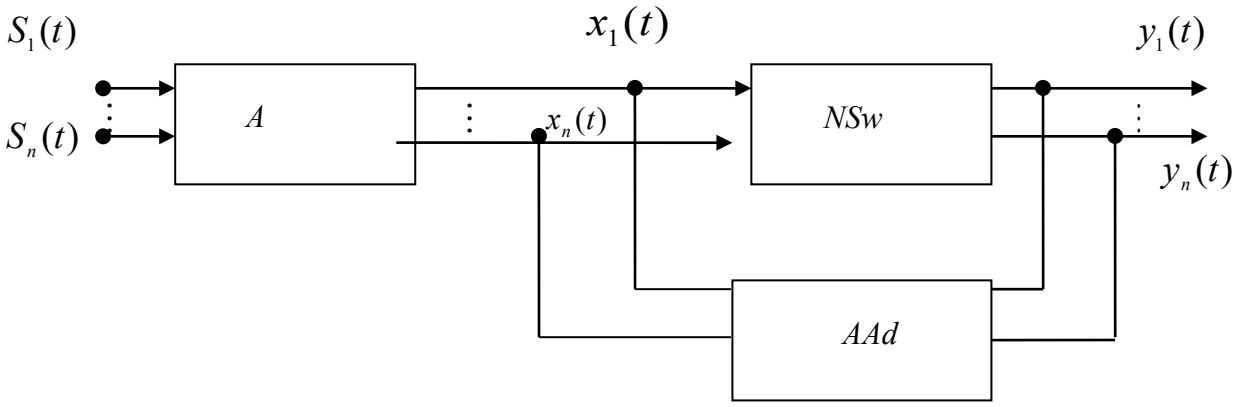


Рисунок 3.4.2 – Схема підключення нейронної мережі

На рисунку 3.4.2. можуть використовуватися такі символи:

— A – матриця змішування;

— NSw - нейронна мережа;

— AAd - алгоритм адаптації.

Для вирішення завдання розподілу сигналів, які є статистично незалежними можна використовувати нейронну лінійну мережу з зворотними зв'язками. Кожен нейрон такої мережі генерує вихідний сигнал відповідно до співвідношення:

$$y_i(t) = x_i(t) - \sum_{j=1,\, j\neq i}^{n} w_{ij} y_j(t).$$

При великій різниці в амплітудах послідовних сигналів, необхідно ввести зворотний зв'язок, яка є власною для нейрона і не дорівнює нулю. Така модифікації адаптаційної залежності, для випадку, якщо $y_{ji}(t)$ не містять постійної складової, записується у вигляді:

$$\frac{dw_{ij}}{dt} \eta\,(t)\; f\;(y_i(t))\; g\;(y_i(t)).$$

Для випадку, коли $i \neq j$, співвідношення запишеться:

$$\frac{dw_{ij}}{dt} = \eta\,(t)[f\;(y_i(t))\; g\;(y_i(t)) - 1].$$

При реалізації рекурентних мереж існують труднощі, які полягають у тому, що практично складно забезпечити стабільність сигналів, особливо, якщо матриця A недостатньо обумовлена, а вхідні сигнали сильно відрізняються між собою. Щоб виключити відповідні складності використовується односпрямована мережа, для якої змішані сигнали $x_i(t)$ складають єдине джерело інформації для мережі.

В рамках теорії нейронної мережі процес навчання відрізняється від процесу самоорганізації тільки тим, що в процесі навчання розглядається як спеціально виділений в часі процес, в якому на входи подаються навчальні вибірки. Алгоритми самоорганізації можуть реалізовуватися в процесі функціонування нейронної мережі, при вирішенні того чи іншого завдання, на яке мережу орієнтована.

3.5. Висновки третього розділу

Отже, в третьому розділі наведені необхідні теоретичні особливості методів навчання нейронних моделей і обрані узагальнені ознаки класифікації нейронних мереж для їх подальшого аналізу.

Розглянуто процес навчання нейронної мережі, сутнісно, являє собою процес формування у мережі таких характеристик, які забезпечували б можливість вирішення завдань, які характерні для систем управління доступом. Проаналізовано типи таких задач і обгрунтований вибір необхідних способів навчання нейронної мережі, яку приймемо в якості базового засобу для моделювання системи доступу.

Прийнято, що система управління доступом, крім завдань управління, вирішує завдання захисту об'єкта, доступом до якого вона управляє. Таким чином, будемо вважати, що така система складається з підсистеми управління доступом і підсистеми захисту об'єкта, доступ до якого забезпечується підсистемою захисту, від атак типу несанкціонованого доступу.

Формалізовано опис атаки для розглянутого випадку і введені визначення успішності атаки (3.1), рівня захищеності об'єкта (3.2), небезпечної і безпечної події (3.3), небезпеки виникнення атаки (3.4) визначені додаткові умови (3.1) і доведено що якщо в системі U_s виділена атака, то на основі аналізу атаки можна сформувати модель загрози, яка відповідною атакою була використана.

Розглянуто методи самоорганізації нейронних систем для вирішення задач розпізнавання атак. І показано що алгоритми самоорганізації можє реалізовуватися в процесі функціонування нейронної мережі, при вирішенні того чи іншого завдання безпеки, на виконання якого мережа орієнтована.

Список використаних джерел до третього розділу

1. Paretto P. On introduction to the modeling of neural networks. Cambridge. Cambridge Univ. Press., 1992.

2. Смарт Н. Криптография / Н. Смарт. – М.: Техносфера, 2005. – 528 с.

3. Богбаш А. В. Криптография / А.В. Богбаш, Г.П. Шапкин. – М.: СОЛОН-Р, 2002. – 512 с.

4. Haykin S. Neural Networks a Comprehensive Foundation. Macmillan College Publishing Company, New York, 1994.

5. Kung S.Y. Digital Neural Networks. Prentice Hall, Englewood Cliffs. N. Jersey 1993.

6. Rosenblatt F. Principles of Neurodinamics. - New York: Spartan Books, 1992.

7. Fausett L. Fundamentals of Neural Networks. Architectures, Algorithms and Applications. Prentice Hall, New Jersey, 1994.

8. Williams R., Zipser D. A learning algorithm for continually running fully recurrent neural networks. Neural Computers, 1989, p. 270-280.

9. Sanger T.D. Optimal unsupervised learning in single layer linear feed formed neural network. Neural networks, 1989, v.2, p.p. 459-473.

10. Давиденко А. Н. Исследование методов обучения нейронных сетей для решения задач противодействия атакам на систему управления доступом / А.Н. Давиденко // Збірник наукових праць Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова. – К.: ІПМЕ ім. Г.Є. Пухова НАНУ, 2007. – Вип. 40. – С. 114-122.

11. Давиденко А. Н. Исследование эффективности применения вероятности применения вероятностных нейронных сетей для решения задачи аутентификации пользователя компьютерных систем / А.Н. Давиденко, Е.А Высоцкая // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : зб. наук. пр. – К., 2004. – Вип. 9. – С. 103-110.

12. Польман Н. Архитектура брандмауэров для сетей предприятия / Н. Польман, Т. Кразес. – М.: Издательский дом «Вильямс», 2003. – 432 с.

13. Лукацкий А. Обнаружение атак / А. Лукацкий. – СПб.: БХВ - Петербург, 2001. – 624 с.

14. Питолин А. В. Основы проектирования искусственных нейронных сетей : учеб. пособ. / А.В. Питолин. – Воронеж: Изд-во ВГТУ, 2001. – 108 с.

15. Kohonen T. Self-organizing maps, Springer Verlag, Berlin 1995.

16. Martinetz M., Berkowich S., Schulten K. Neural-gas network for vector quantization and its application to time series prediction. Trans. Neural Networks, 1993, v. 4, p.p. 558-569.

РОЗДІЛ 4. ДОСЛІДЖЕННЯ МЕТОДІВ ФОРМУВАННЯ КОМПОНЕНТ СИСТЕМ РОЗМЕЖУВАННЯ ДОСТУПУ

4.1. Аналіз основних інформаційних компонент систем розмежування доступу

Системи розмежування доступу реалізують взаємозв'язок між об'єктом доступу і користувачем засобів, які представляє об'єкт користувачеві. В цьому випадку, такий взаємозв'язок реалізується у вигляді інтерфейсу між користувачем і об'єктом доступу. У більшості випадків, дані, якими оперує об'єкт, не мають форми відображення, яка збігалася б з даними, якими оперує користувач, особливо якщо таким користувачем є не процес, а людина, що вирішує свою прикладну задачу. Тому, система розмежування доступу, яка обмежується лише функціями інтерфейсу, повинна мати досить розвиненою інформаційною структурою. Така інформаційна структура необхідна для вирішення завдань перетворення області інтерпретації даних користувача, які представлені у відповідній формі, в форму, яка прийнятна для об'єкта доступу. Відповідна система розмежування доступу повинна здійснювати і зворотні перетворення форм представлення даних. Очевидно, що відповідні перетворення форм представлення даних тісно пов'язані з описами предметних областей інтерпретації, якими користується користувач і областей, інтерпретації, які допустимі в об'єкті доступу. Якщо взяти до уваги, що таких користувачів з різними областями інтерпретації їх прикладних задач у одного об'єкта доступу може бути багато, то стає очевидною досить велика складність вирішення завдання перетворень одних форм представлення даних в іншу і навпаки. У сучасних системах розмежування доступу завдання перетворення вхідних даних в необхідну для об'єкта форму розподілена за всіма складовими, які використовують систему доступу. Таким чином, для системи розмежування доступу виділена лише частина функціональних перетворень, які вирішують задачу узгодження даних, що виходять від користувача до об'єкта доступу і

навпаки. До таких завдань, які визначені для системи розмежування доступу, можна віднести наступні:

— завдання надання користувачеві спадкоємного інтерфейсу;

— вихідне перетворення даних користувача в форму подання прийнятну для об'єкта;

— перетворення даних, що надходять від об'єкта доступу до користувача, в форму прийнятну для окремого користувача;

— формування додаткових коментарів до даних, призначеним окремому користувачеві, якщо користувачем є людина і останній сформував запит про таких коментарі;

— завдання ідентифікації користувача, метою вирішення якої є визначення окремого користувача, якщо таких користувачів може бути більше одного.

Наведені вище завдання це класичний набір функцій системи доступу, для випадку, коли не розглядаються завдання безпеки системи доступу, об'єкта доступу і забезпечення безпеки користувачів, які використовують відповідну систему розмежування доступу (*SRD*).

Для вирішення завдань безпеки *SRD*, Для зручності, будемо говорити про безпеку *SRD* маючи на увазі безпеки всіх перерахованих складових, необхідна досить розвинена система інформаційного забезпечення тих підсистем, які безпосередньо орієнтовані на вирішення завдань захисту всіх компонент *SRD*. При коректному проектуванні *SRD*, причинами зміни рівня безпеки можуть бути, в першу чергу, зовнішні фактори, які можуть впливати на роботу *SRD*. Внутрішні чинники, які теж можуть негативно впливати на роботу *SRD* розглядати не будемо, так як до них будемо відносити такі чинники як виникнення несправності або виникнення дефектів, що впливають на штатні режими роботи *SRD*. Оскільки зовнішні фактори впливають негативно на *SRD* ініціюють відповідні дії недетерминировано, то характерним для вирішення завдань захисту *SRD* є такі методи:

— методи прогнозування виникнення атак *SRD* з боку зовнішніх небезпек;

— методи адаптацій *SRD* до зовнішніх умов, в яких функціонує *SRD*;

— методи розпізнавання негативних зовнішніх впливів на *SRD* або розпізнавання атак;

— методи визначення поточного рівня безпеки окремих компонент і системи *SRD* в цілому;

— методи протидії атакам, які були виявлені на різних етапах їх реалізації, включаючи кінцевий етап реалізації атаки, якщо остання є успішною.

З наведених базових методів вирішення завдань забезпечення безпеки видно, що для їх реалізації і ініціації не існує або досить складно визначити детермінований набір вхідних даних, які забезпечували б можливість однозначно визначити алгоритм реалізації відповідних методів вирішення задач, які в сукупності вирішували б завдання забезпечення безпечного функціонування системи *SRD*. У зв'язку з цим, доцільно для вирішення наведених завдань використовувати кошти, які в максимально можливій мірі були б придатні для реалізації наведених вище методів вирішення окремих складових завдання забезпечення безпеки функціонування системи *SRD*. На основі з раніше проведеного аналізу можливостей нейронних мереж, як засобів вирішення завдань розпізнавання, адаптації до постійно змінюваних зовнішніх впливів, які можуть бути основою для вирішення завдань прогнозування змін у зовнішніх впливах, а також ряду інших завдань, включаючи завдання визначення рівня безпеки і завдання ініціації засобів протидії атакам, в даній роботі в якості універсальних засобів вирішення завдання безпеки *SRD* в цілому, обрані засоби, які реалізуються на основі використання нейронних мереж.

Однією з важливих особливостей використання системи різних типів нейронних мереж є необхідність у використанні досить розвиненою інформаційної системою, яка відображала б всі необхідні для функціонування нейронних систем дані. Крім того, в рамках відповідної інформаційної системи повинні існувати засоби, які забезпечували б попередню обробку відповідних даних, перш ніж останні можна було б подавати у функціональні блоки, які реалізовані на основі використання нейронних мереж. Цілком очевидно, що інформаційна система (*IS*) повинна ґрунтуватися на описах предметних областей,

які описують інтерпретацію даних, які використовуються в усіх фрагментах SRD. Тому розглянемо основні компоненти IS, які необхідні для вирішення завдань інформаційного забезпечення системи безпеки SRD, яку скорочено будемо позначати символами BSD. До таких компонентів віднесемо наступні:

— словники, що містять опис базових елементів предметних областей (S_C);

— система синтаксичних правил формування описів інтерпретації базових елементів (Ω);

— система семантичних параметрів, які характеризують особливості інтерпретації базових елементів і інших компонентів BSD (Λ);

— система семантичних правил, які регламентують способи побудови опису інтерпретації елементів, які використовуються при функціонуванні системи BSD;

— система правил перетворення описів компонент системи BSD (Σ).

Словники є описами ідентифікаторів і інших компонент, які використовуються в SRD. Оскільки предметні області з боку користувачів або зовнішні предметні області можуть мати різний рівень абстракції, то немає сенсу прив'язуватися до одного з можливих мов, яким могла б описуватися окрема предметна область. В даному випадку зміна рівня абстракції мови визначається кількістю нових базових ідентифікаторів, які вводяться в якості позначення реальних об'єктів або факторів, які мають своє самостійне значення в деякій предметній області інтерпретації. Прикладом такого типу зміни рівня абстракції в описі предметної області може служити використання професійної термінології. При цьому, така термінологія може бути ще й не загальноприйнятою. В цьому випадку, відповідну термінологію називають жаргоном. Отже, найбільш низьким рівнем абстракції буде володіти мовою, який будується на основі базових компонент, що описують найбільш широко поширену предметну область. При використанні такого способу визначення зміни рівня абстракції мови, може мати місце ситуація, коли дві різні предметні області, які використовують різні базові елементи по відношенню один до одного, мають максимальний рівень абстракції.

Для виключення можливості виникнення такої суперечливості, приймемо такі умови.

Умова 4.1. Вимірювання зміни рівня абстракції можливо тільки між двома описами предметних областей, які мають не менше половини загальних базових елементів.

Умова 4.2. Вимірювання величини зміни рівня абстракції можливо тільки між двома послідовно модифікованими описами предметних областей.

Умова 4.3. Зміна величини рівня абстракції між двома послідовно розглядаються описами предметної області не може перевищувати 10% від загальної кількості базових елементів який модифікується опису предметної області.

Беручи до уваги, що опис предметної області являє собою словник S_C, о наведені вище умови можна описати формально. Для цього приймемо, що послідовне перетворення S_C, яке призводить до зміни рівня абстракції певного опису предметної області, в загальному вигляді запишеться наступним співвідношенням:

$$A(S_C) = \{S_{C1} \to [F_{A1}(S_{C1}) = S_{C2}] \to ... \to [F_{A(n-1)}(S_{C(n-1)})] \to S_{Cn} \qquad (4.1)$$

де F_{Ai} - перетвореня S_{Ci}, яке призводить до збільшення рівня абстракції опису предметної області S_{Ci}. У цьому випадку умова 4.1 запишеться у вигляді наступного співвідношення:

$$[S_{Ci} \cap S_{C,(i+1)} = 1/2(S_{Ci} \,\&\, S_{C,(i+1)})] \to U_{Ai}[F_{Ai}(S_{Ci})] \qquad (4.2)$$

де U_{Ai} - функція визначає величину зміни рівня абстракції в $S_{C(i+1)}$, Який реалізується співвідношенням $F_{Ai}(S_{Ci}) \to S_{C,(i+1)}$.

Умова 4.2 формально описується наступним співвідношенням:

$\Delta Q_i = Q_{Ai}[S_{Ci}, F(S_{Ci})]$, де ΔQ_i - величина зміни рівня абстракції в $S_{C,(i+1)}$ по відношенню до S_{Ci}.

Умова 4.3 формально записується у вигляді наступного співвідношення:

$Q_{Ai}(S_{C,(i+1)}) \le 0{,}1 \,|\, S_{Ci} \,|$,

де $|S_{Ci}|$ - параметр, що характеризує S_{Ci} і який використовується для обчислення $Q_{Ai}(S_{Ci})$. У найпростішому випадку, цей параметр являє собою потужність множини S_{Ci}.

Умови 4.1 і 4.2 передбачають використання однієї і тієї ж предметної області, яка допускає на окремому етапі модифікації свій розвиток. Якщо ці умови не виконуються, то відповідні S_{Ci} і S_{Cj} являються різними. В рамках прийнятого підходу до оцінки рівня абстракції опису S_{Ci} відсутня можливість порівнювати по параметру рівня абстракції S_{Ci} з S_{Ci+j}, якщо $j \geq 2$. аким чином, співвідношення (4.1) описує деяку еволюцію розвитку S_{Ci}, Яка відбувається протягом змін S_C з S_{C1} до S_{Cn}. Оскільки опис предметної області S_C є базовим, для роботи системи BSD, То необхідно більш повно розглянути S_C, Всі процеси, які можуть відбуватися в рамках S_C і процеси, які пов'язані з перетвореннями самих словників S_C. Очевидно, що відповідні процеси повинні описуватися параметрами, які їх характеризують. До таких процесів віднесемо наступні зміни і модифікації, які можуть відбуватися в S_C:

- процеси зміни рівня абстракції в описі предметної області, $A(S_C)$;
- процеси еволюційного розвитку S_C, $(E(S_C))$;
- процеси локальних модифікацій S_C, $(M(S_C))$;
- процеси виродження S_C, $(V(S_C))$;
- процеси деградації S_C, $(D(S_C))$;
- стабілізуючі процеси в S_C, $(C(S_C))$;
- катастрофічні процеси в S_C, $(K(S_C))$.

Процеси зміни рівня абстракції описуються в загальному випадку співвідношенням (4.1) і формальними уявленнями умов 4.1-4.3. Такий параметр, як рівень абстракції S_C, який будемо позначати символом μ, являє собою характеристику одноразового перетворення $S_{Ci} \to S_{C(i+1)}$.

Процеси еволюційного розвитку S_C охоплюють цілий ряд перетворень семантичного словника S_C і, в загальному випадку, можуть бути представлені у вигляді наступного співвідношення:

$$E(S_C) = \{f_1[S_{C1}, d_1(t)] \to f_2[S_{C2}, d_2(t)] \to ... \to f_n[S_{Cn}, d_n(t)]\},$$

де f_i - функція, яка описує перетворення в словнику S_C з урахуванням інтерактивної взаємодії з системою доступу, яка розширена підсистемою безпеки доступу, $d_i(t)$ - інтерактивна взаємодія користувача, який використовує опис предметної області S_{Ci}, t - час реалізації відповідної взаємодії. Очевидно, що цей процес $E(S_C)$ повинен оцінюватися критеріями, які визначають його, як еволюційний процес. Всі процеси, які можуть відбуватися в S_C, Ініціюються користувачем, при цьому, користувач може бути санкціонованим і несанкціонованим. Природно припустити, що всі процеси, які відбуваються в S_C, Описуються параметрами, значення яких відрізняються між собою в разі їх ініціалізації санкціонованими користувачами і несанкціонованими користувачами. Більш того, процеси ініційовані несанкціонованим користувачем, можуть призводити до ситуацій, які є неприпустимими, що визначається наступними факторами, які виникають в S_C:

— суперечливістю, що виникає в S_C і що виявляється в різних формах (μ_e);

— конфліктами між компонентами S_C, що виникають в результаті несанкціонованої ініціації процесів в S_C, (η_e);

— порушення процесу функціональних перетворень, які регламентовані вище наведеними типами процесів і можуть складатися в циклічних модифікаціях S_C, в дублюванні елементів S_C і інших проявах відповідних порушень (χ_e).

Еволюційність процесів в довільних об'єктах визначається по відношенню до навколишнього середовища, в якій відповідний об'єкт функціонує. У цьому випадку, навколишнє середовище для S_C зводиться до системи доступу, з якою

взаємодіє S_C за допомогою ініціації користувачем взаємодії з системою доступу. Тому критерії еволюційності процесів повинні характеризувати збільшення рівня безпеки. У загальному випадку, рівень безпеки доступу характеризується деяким центральним параметром системи доступу, який враховує всі фактори, що впливають на рівень безпеки. В даному випадку, розглянемо цей параметр тільки в частині, яка враховує фактори, пов'язані з S_C. Фактори, які відображають зміну рівня безпеки приведені вище. Ці фактори мають наступну особливість. Оскільки їх поява обумовлюється діями несанкціонованого користувача, то останній не ініціює безпосередніх змін в S_C, а здійснюючи несанкціонований доступ до об'єкта, і в разі його виявлення, дає підставу зовнішнім по відношенню до S_C компонентів, інтерпретувати дані, які він використовував, як такі, що належать S_C. Таким чином, можна прийняти, що еволюційний процес у S_C має місце, якщо $[\gamma = \mu_e + \eta_e + \chi_e] \to \min(\gamma)$. Для спрощення розгляду, приймемо, що все μ_e, η_e і χ_e є рівноцінними з точки зору їх впливу на рівень безпеки і будемо їх позначати одним символом ξ_i.

Процеси локальних модифікацій S_C або $M(S_C)$ найчастіше пов'язані з необхідністю з боку легального користувача, розширити можливості в отриманні ресурсів з об'єкта доступу. Незважаючи на те, що така модифікація проводиться легальним користувачем, вона може привести до виникнення факторів типу ξ_i, особливо якщо S_C вже розширювалася на попередніх етапах функціонування системи: $P \leftrightarrow SD \leftrightarrow OD$, где P - користувач, OD - об'єкт доступу.

Процеси виродження $V(S_C)$ являють собою такі перетворення в S_C, Які призводять до зменшення можливого різноманітності при формуванні запитів на обслуговування. Визначення величини параметра, який характеризує процес деградації, досить складно, оскільки просте зменшення компонент в S_C не приводить до зменшення можливих запитів до системи SD. Запити, які можуть формуватися на основі даних з S_C, будемо позначати z_i. Для формування запитів z_i крім даних з S_C, Використовуються системи виведення нових формул

запиту, яка включає в себе систему правил формування семантичних правильних формул Ω ісистему семантичних правил $P\Lambda$, що формально можна записати в такий спосіб:

$$[S_C, \Omega(S_C), P\Lambda(S_C), \Lambda] \to z_i \qquad (4.3)$$

Перш ніж в конструктивному вигляді представляти співвідношення (4.3), розглянемо на якісному рівні інші процеси.

Процеси деградації $D(S_C)$ відрізняються від процесів $V(S_C)$ тим що $D(S_C)$ не призводять до зменшення кількості елементів в S_C, а лише призводять до зменшення кількості запитів, які можуть бути виведені на основі використання S_C. Оскільки z_i у співвідношенні з (4.2) залежить не тільки від S_C, то розглянемо, які перетворення в S_C можуть вплинути на можливість виведення z_i з Σ, де $\Sigma = \{S_C, \Omega(S_C), P\Lambda(S_C), \Lambda\}$. Оскільки кількість елементів в S_C у результаті $D(S_C)$ не зміниться, то $D(S_C)$ має впливати на $\Omega(S_C)$ і $P\Lambda(S_C)$, Або хоча б на одну з цих компонент. Оскільки $P\Lambda$ і Ω являють собою системи правил, то процеси $D(S_C)$ здійснюють таке перетворення $(\Omega \& P\Lambda) \vee \Omega \vee P\Lambda$, яке унеможливлює їх використання при виведенні z_i. Цей фактор проявляється в тому випадку, якщо відповідні x_i з S_C змінюють свої інтерпретаційні опису $T(x_i)$ таким чином, що $\Omega(S_C)$, або $P\Lambda(S_C)$ або $(\Omega(S_C) \& P\Lambda(S_C))$ стають суперечливими, при реалізації співвідношення (4.2) або процедура z_i приводить до конфліктної ситуації в процесі $L_i(S_C, \Omega(S_C), P\Lambda(S_C), \Lambda) \to z_i$, де L_i - функція логічного висновку z_i.

Стабілізуючі процеси $C(S_C)$ представляють альтернативу для процесів дестабілізуючих, до яких можна віднести процеси $V(S_C)$ і $D(S_C)$. Справа в тому що $V(S_C)$ і $D(S_C)$ можуть ініціюватися зовнішніми, по відношенню до SD факторами, з метою компрометації SD або з метою реалізації атаки на SD. Таким чином, $C(S_C)$ являє собою процес протидії вторгненню в систему SD. Оскільки наслідком дестабілізації, до якої призводять $V(S_C)$ і $D(S_C)$, являє собою виникнення в S_C суперечливих і конфліктів, то $C(S_C)$ повинен їх

усувати. Очевидно, що ініціація такого здійснюється не тільки в разі, коли необхідний z_i виявляється не виводяться, а й у разі реалізації процесів визначення рівня безпеки системи BSD в цілому. Ці процеси реалізуються відповідно до алгоритмів забезпечення заданого рівня безпеки системи доступу в цілому. Як уже зазначалося, під безпечною системою доступу будемо мати на увазі трійку $BSD =< P, SD, OD >$.

Катастрофічні процеси $K(S_C)$ представляють собою процеси, яким в рамках BSD еможливо протидіяти. Всі розглянуті процеси уявляють собою певні послідовності перетворень, в даному випадку, перетворень в S_C. Оскільки дестабілізуючими процесами є $V(S_C)$ і $D(S_C)$, то формально, для визначення $K(S_C)$ можна записати співвідношення:

$$\{\{[V(S_C) \& D(S_C)] \vee \Phi[V(S_C), D(S_C)]\} \& \neg C(S_C)\} \to K(S_C),$$

де Ф – функція організації взаємодії між $V(S_C)$ і $D(S_C)$. Заперечення перед $C(S_C)$ означає, що $C(S_C)$ не може протидіяти санкціонованим змінам в S_C.

4.2. Опис семантики окремих компонент системи розмежування доступу

Система розмежування доступу в значній мірі ґрунтується на інформаційних елементах. Особливістю інформаційних елементів є їх залежність від опису їх інтерпретації $T(x_i)$, где x_i - інформаційний елемент, $T(x_i)$ - опис його інтерпретації. Базовими складовими інформаційних компонент є пропозиції або фрази мови, який використовується для формування $T(x_i)$. У більшості випадків, як такої мови вибирається природна мова, особливо, якщо мова йде про систему за участю користувачів. Тому, важливими компонентами інформаційних засобів є синтаксис і семантика відповідної мови. Розглянемо ці компоненти в рамках обмежень, які випливають з особливостей і завданнями системи безпеки доступом BSD.

Оскільки, базовими засобів і аналізу безпеки, рівень якої визначаєтьсяється в рамках SRD, є нейронні мережі, то описи які використовуються в системі доступу,

повинна допускати свою кількісну інтерпретацію. Окремі інформаційні компоненти взаємопов'язані між собою. Тому, для коректного їх опису, необхідно розглянути структуру організації відповідних компонент. До складу такої структури входитимуть не тільки словник S_C, синтаксичні та семантичні правила Ω і $P\Lambda$, семантичні параметри Λ і правила перетворення інформаційних компонент Σ, але і об'єкти, які складають опис предметних областей, в яких вирішуються завдання забезпечення безпеки SRD. До таких компонентів можна віднести:

— компоненти опису предметних областей, які відображають інтереси користувачів і, для зручності, вони будуть ідентифікувати окремих користувачів, позначати їх будемо символом U_i;

— засоби захисту в частині їх інформаційного забезпечення IZ, які входять до складу системи BSD;

— підсистема інформаційного забезпечення об'єкта доступу IOD.

На рисунку 4.1 зображена структурна схема засобів інформаційного забезпечення системи безпеки системи доступу до об'єкта доступу. На рисунку використовуються наступні позначення:

— $PIOSD-i$ - підсистема інформаційного забезпечення системи доступу;

— $PIOPO-i$ - підсистема інформаційного забезпечення предметної області користувача;

— PSP - підсистема семантичних ознак;

— PCP - підсистема семантичних правил;

— $IOSZ$ - інформаційне забезпечення засобів захисту об'єкта доступу;

— PPS - підсистема синтаксичних правил;

— PPV - підсистема правил виведення;

— SS - семантичний словник;

— PUB - підсистема управління безпекою.

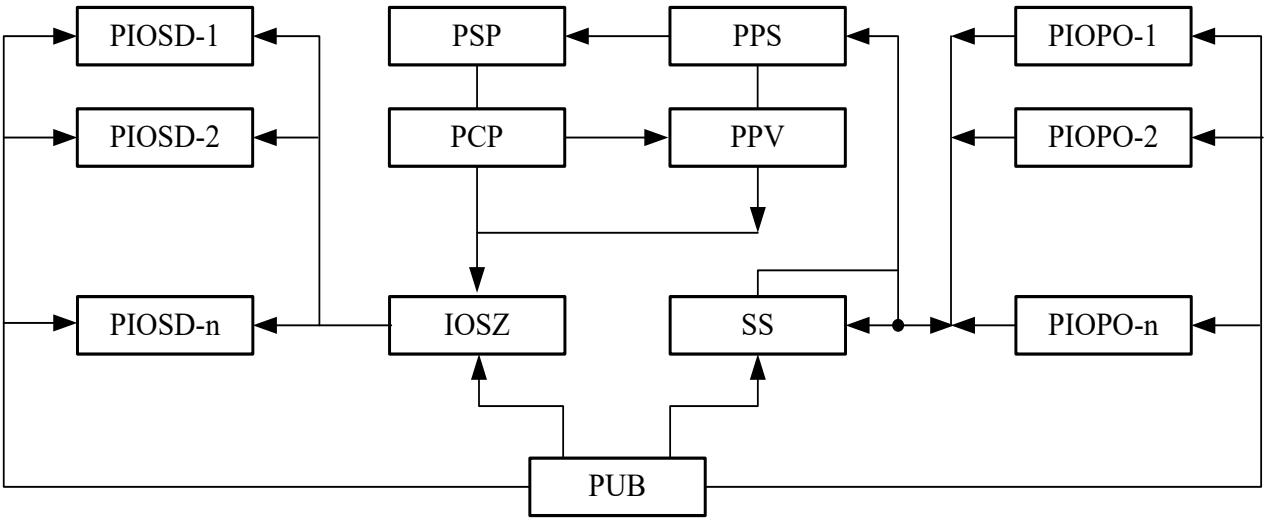


Рисунок 4.1 – Структурна схема засобів інформаційного забезпечення системи розмежування доступу SRD.

Підсистема $PIOSD-i$ містить опис предметної області системи розмежування доступу. Предметна область системи розмежування доступу являє собою опис всіх коштів, які використовуються або можуть використовуватися для вирішення завдань безпосередньо пов'язаних з реалізацією доступу користувача до об'єкта доступу і засобів або опису предметної області, яке пов'язане з вирішенням завдань забезпечення безпеки системи доступу. Оскільки перша група завдань дуже тісно переплітається з другою групою завдань, то будемо розглядати завдання зі згаданих груп під кутом зору забезпечення безпеки системи доступу. Природно припустити, що міра розширення засобів захисту в системі доступу впливає на величину безпеки функціонування відповідної SRD. Тому розглянемо засобі, які можуть використовуватися в рамках SRD, для забезпечення безпеки функціонування системи. До таких засобів, які відповідають різним аспектам забезпечення безпеки і відображають різні підходи до забезпечення безпеки системи доступу в цілому, можна віднести наступні:

— засоби ідентифікації користувача (SIP);

— кошти аутентифікації користувача на основі різних інформаційних підходів (SAI);

— кошти аутентифікації на основі поділу таємної інформації (SAT);

— кошти виявлення аномалій в SRD на основі використання нейронних мереж (VAN);

— виявлення аномалій в SRD на основі імовірнісних моделей (VAV);

— засоби контролю доступу на основі використання різних моделей доступу (SKD) та інш.

Кожниї з наведених вище засобів, по суті, являє собою окремий фрагмент предметної області системи SRD розширеної до системи BSD. Очевидно, що кожної окремої SRD немає необхідності використовувати всі існуючі засоби для забезпечення безпеки SRD, оскільки, вимоги до рівня безпеки для різних SRD можуть бути різними. У зв'язку з цим, необхідно вирішити задачу визначення і розробки методів і розробки оцінки рівня безпеки, який забезпечується кожним окремим засобом.

Другим важливим завданням є завдання встановлення взаємозв'язків між окремими засобами. На підставі таких взаємозв'язків можна будувати впорядковану структуру системи BSD, в яку входять окремі засоби безпеки. В рамках цієї структури упорядкування може вестися по відношенню до величини безпеки, яку забезпечує кожний із засобів.

Третім завданням, яке необхідно вирішувати, це побудова для кожного з засобів або для кожного фрагмента відповідної області предметної інтерпретації індивідуальні інформаційні розширення, за допомогою яких можна пов'язувати між собою засоби захисту різних типів. Справа в тому, що кожний із засобів володіє власною специфікою вирішення завдань захисту, яка описується відповідною моделлю. Щоб специфіки різних засобів пов'язати між собою, необхідно використовувати не тільки їх інформаційні розширення, а й інформаційні моделі відповідних коштів, оскільки, тільки на інформаційному рівні можна реалізувати взаємозв'язки між різними типами математичних моделей засобів захисту системи доступу.

Черговою задачею, яку необхідно вирішувати і яка безпосередньо пов'язана з попередніми завданнями, є завдання формування формальних засобів опису інформаційних моделей, що дозволить здійснювати необхідні узагальнення побудованих інформаційних моделей. Таке узагальнення дозволить спростити методи вирішення завдань формування структури системи захисту, в яку може входити цілий ряд окремих засобів захисту SRD.

Перш за все, коротко розглянемо основні уявлення про типові які широко використовані засоби захисту. Першим з таких засобів захисту є засіб ідентифікації користувача SIP. На сьогоднішній день можна прийняти наступні класи методів ідентифікації [1]:

— ідентифікація на основі використання паролів IP;

— сильна ідентифікація на основі використання принципу «дзвінок - відповідь», який будемо позначати (ZO);

— ідентифікація на основі використання протоколів та схем ідентифікації (IS);

— найбільш повна ідентифікація реалізується на основі використання електронного підпису (ICP).

Найнижчий рівень захисту у засобів ідентифікації, які використовують паролі. У цьому випадку основним елементом IP є список паролів, які, найчастіше, зберігаються в зашифрованому вигляді. В цьому випадку ідентифікація полягає в розпізнаванні пароля, який надсилає користувач в систему доступу.

Сильна ідентифікація на відміну від IP здійснюється шляхом реалізації обміну між SD і PO. Формально, таку схему можна описувати таким чином:

1) $A \to B : r_A$.

2) $B \to A : \{A, r_A, r_B\}_K = A_K(A, r_A, r_B, k_i)$

3) $A \to B : \{B, r_B, \}_K = A_K(B, r_B, k)$

Де $\{A, r_A, r_B\}$ зашифроване ключем k повідомлення, $\{A, r_A, r_B\}$, r_A і r_B - випадкові числа, А і В дві сторони, між якими реалізується ідентифікація.

Важливі інформаційні компоненти такої схеми є: опис генератора псевдовипадкових чисел, опис ключа шифрування k і опис що використовується алгоритму шифрування переданих повідомлень. Основними факторами захисту, в даному випадку, є псевдовипадкові числа r_A і r_B і відповідний генератор, а також алгоритм шифрування повідомлень, який використовує ключ k.

Ідентифікація, заснована на використанні протоколів і схем, які ґрунтуються на складності рішення задач факторизації великих чисел, забезпечують досить високий рівень захисту від проникнення до OD несанкціонованого користувача. Такі протоколи для своєї реалізації вимагають використання сертифікаційного центру. Як приклад розглянемо протокол ідентифікації FFS [2].

Перед використанням цього протоколу, центр сертифікації CS формує два простих числа p і q такі, щоб мали місце співвідношення:

$$p = 3 \bmod 4, q = 3 \bmod 4$$

Ці числа CS містить в секреті, а публікує твір $N = p * q$. Після цього учасники обміну виконують реєстрацію в CS, яка полягає в наступному і стосується користувача:

— користувач вибирає l випадкових цілих чисел $S_1,...,S_l \in Z_N^*$;

— вибирає випадковим чином бітовий вектор $(e_1,...,e_l)$;

— користувач обчислює числа ω_i на основі співвідношень: $\omega_i = (-1)^{e_i} (S_i)^{-2} \bmod N$, для $i = 1,...,l$;

— користувач реєструє в CS вектор $(\omega_1,...,\omega_l)$, як свою ідентифікаційну інформацію, при цьому, користувач зберігає в таємниці вектор $(S_1,...,S_l)$.

На етапі ідентифікації користувача в системі доступу, користувач ілюструє SD факт володіння інформацією про вектор $(S_1,...,S_l)$, реалізуя t- кратно наступні послідовності дій:

1) $P \to SD : U = r^2 \bmod N$, де $r \in Z_N^*$

2) $SD \to P : (b_1,...,b_l) \in \{0,1\}^l$

3) $P \to SD : \upsilon = r П_{i=1}^{l} (S_i)^{bi} (\bmod N)$

4) Ідентифікація завершується підтвердженням автентичності користувача, якщо виконується співвідношення:

$$U = \pm\upsilon^2 \Pi_{i=1}^{l}(\omega_i)^{bi} (\mathrm{mod}\, N).$$

В даному випадку рівень захисту, який може забезпечуватися відповідним протоколом залежить від величини вектора $(\omega_1,...,\omega_l)$, під яким зареєструвався користувач в центрі сертифікації. Складність завдання факторизації, в свою чергу, визначається величинами простих чисел, які вибираються для визначення величини модуля, відповідно до якого реалізуються обчислення.

Використання цифрового підпису в системах ідентифікації детально розглядати не будемо, оскільки електронний підпис відрізняється від схеми ідентифікації заміною верификатора функціями хеширования, які формують хеш-образи окремих даних. Для формування систем ідентифікації і аутентифікації користувачів також використовуються математичні моделі, які ґрунтуються на окремих теоретичних засадах. Прикладом такої моделі і відповідного теоретичного обґрунтування є модель, яка побудована на основі використання теорії ігор [3]. В рамках математичних засобів теорії ігор існує можливість реалізовувати різного типу атаки на систему доступу. До таких атак відносяться:

— атака підміни санкціонованого користувача;

— атака фальсифікації повідомлень;

— атака підслуховування повідомлень.

У моделях цього типу, в якості партнерів гри, виступає система доступу і, відповідно, система захисту доступу спільно з санкціонованим користувачем і з іншого боку, партнером гри є несанкціонований користувач, яких будемо відповідно позначати SP і NP. Вихідними даними для побудови моделі системи захисту доступу є:

— перший гравець являє собою дві сторони що обмінюються OD і SP;

— другий гравець є NP;

— повідомлення представляється як безліч станів джерела повідомлень $S = \{S_1,...,S_n\}$;

— для приховування S_i використовується система правил кодування $E = \{e_1,...,e_m\}$.

В рамках цих позначень безліч ідентифікаторів $T = \{t_1,...,t_m\}$ формується відповідно до співвідношення $t = e(S)$, безліч криптограми, яке складається з $M = \{m_1,...,m_n\}$ формується на основі співвідношення $m = (S,t)$. В цьому випадку, код що ідентифікує, який називається А-кодом, являє собою набір з $< S,M,E >$. Криптограма, яка використовується для передачі повідомлення, це відкрите повідомлення S_i і ідентифікатор t. Система доступу від SP отримує $m' = (S',t')$ і здійснює перевірку ідентифікатора шляхом обчислення $t^* = e(S')$. Якщо виявиться, що має місце $t^* = t'$, то повідомлення справжнє або джерелом повідомлення є SP. Якщо NP хоче підробити повідомлення S, то він повинен вгадати справжнє значення t, яке використовує SP. Для вирішення завдання підробки з боку NP і завдання захисту каналу $(SP \to OD)$ використовується модель теорії ігор, яка відноситься до класу ігор зі змішаними стратегіями. Природно припустити, що досягнення мети з боку NP може бути здійснено на основі реалізації послідовних спроб підібрати необхідну мітку t_i. Протидія відповідної атаці полягає в послідовних змінах t_i на t_j з T в процесі реалізації пересилань даних або повідомлень S_i. Такі послідовності називаються стратегіями для NP і $(SP \to OD)$, відповідно. Методи вирішення завдань, в рамках ігор зі змішаними стратегіями, дозволяють досліджувати можливість побудови таких стратегій, які можуть привести до досягнення цілей з боку NP або з боку $(SP \to OD)$. Зрозуміло, що NP знає в кожному випадку m_i і t_i. Як правило, t_i формується на багатьох значень $\{0,1\}$ і тому відповідна матриця, при моніторингу каналу $(SP \to OD)$ користувачем NP, може виявитися відомою. Елементами такої матриці А являються біти 0 або 1, які вибираються стороною $(SP \to OD)$ у відповідності з тільки їм відомими правилами e_i. Тоді рядки матриці відповідають правилам e_i із E, а стовпці повідомленнями m_i фз M. Вибір стороною $(SP \to OD)$ на черговому кроці обміну

e_i для обчислення t_i визначається ймовірністю $P(e_i)$. В цьому випадку, міра успіху сторони NP може бути представлена співвідношенням:

$$P_{ОП} = \max \sum_{m \in M} \eta_{\text{m}} (\sum_{e \in E} П_{\text{e}} a_{em}),$$

де η_m це можливість вибору для криптограми m_i ідентифікатора a_m, $Ï_e$ - один крок стратегії з боку NP. У цьому випадку, відповідно до базових положень теорії ігор оптимальна стратегія для $(SP \to OD)$ протидіюча стратегії NP, складається в мінімізації $P_{ÎÏ}$, що формально запишеться:

$$\text{P}^*_{\text{ОП}} = \min(\max \sum_{m \in M} \sum_{e \in E} П_{\text{e}} \eta_m a_{em}).$$

Аналогічно, умовну ймовірність досягнення успіху з боку, при реалізації певної стратегії вгадування ідентифікаторів, можна записати у вигляді співвідношення:

$$P^*_{O\eta} = \max(\min \sum_{m \in M} \sum_{e \in E} П_{\text{e}} \eta_m a_{em}).$$

Елементи a_{em} прийнято називати елементами матриці успішної гри.

Наведені вище опису представляють собою різні приклади предметних областей, в яких реалізуються механізми контролю доступу. У зв'язку з цим, необхідно таким чином сформувати фрагменти семантичних словників для відповідних предметних областей, щоб виявилося можливим вирішення завдань захисту не тільки в рамках певної реалізації одного з варіантів алгоритму контролю доступу, але і було можливо на основі аналізу семантики відповідних описів розширювати і модифікувати відповідні алгоритми доступу. Оскільки семантичний словник S_C, в основному, являє собою опис, який використовується для відображення інтерпретаційних розширень на природній мові, то, в загальному вигляді, один елемент словника можна представити таким чином:

$$x_i = < a_{i1}, a_{i2} ..., a_{in} > | < a_{k1}, a_{k2}, ..., a_{km} > | ... < a_{j1}, ..., a_{jk} >$$

де $< a_{j1}, ..., a_{jk} >$ окремий фрагмент текстового опису інтерпретаційного розширення для x_i, a_{ij} - окреме слово відповідного фрагмента. Фрагментом $\varphi_i(a_{i1}, ..., a_{in})$ може служити фраза, пропозиція або інша конструкція, яка визначається синтаксичними схемами.

Для випадку схем сильної ідентифікації окремі елементи предметної області можуть в рамках семантичного словника описуватися наступним чином:

$SP =<$ санкціонований користувач $>$

$\mathrm{NP} =<$ несанкціонований користувач $>$

$SD =<$ система доступу $>$

$(r_1,...,r_n) =<$ випадкові числа, n$>$

$K =<$ ключ криптографічний $>$

$(A_1,..., A_k) =<$ алгоритми криптографічні блокові, k$>$

$A_1 =< x_1(A_1) >\rightarrow \{$ опис блочного алгоритму $A_1\}$

$A_m =< x_m(A_m) >\rightarrow \{$ опис блочного алгоритму $A_m\}$

$S_1 =< x_1(S_1) >\rightarrow \{$ опис схеми доступу $S_1\}$

$S_k =< x_k(S_k) >\rightarrow \{$ опис схеми доступу $S_k\}$

У наведеному вище фрагменті семантичного словника присутній приклад опису предметної області. Такі інтерпретаційні розширення, як $< x_i(A_i) >$ и $< x_i(S_i) >$, являють собою скорочені опис алгоритму і схеми доступу, яке використовується тільки в рамках наведеного прикладу опису фрагмента опису S_C.

Використання семантики, в традиційних підходах, обмежується автоматизацією процесів відображення необхідної для користувача інформації при формуванні дружнього інтерфейсу. У цьому випадку, функції семантики розглядаються значно ширше. Це розширення орієнтоване на обгрунтування можливості використання особливостей семантики об'єктів, які досліджуються, для опису, спеціальних семантичних параметрів, які дозволяють проводити кількісний аналіз семантичних чинників. У зв'язку з цим, виникає необхідність, на певному рівні семантичних описів, перейти від особливостей відображення семантики до формальних оцінками відповідних особливостей. Головними особливостями семантичних описів є наступні:

— якісний характер таких описів;

— наявність кількісної невизначеності, яка відображається у відповідних описах;

— суб'єктивність уточнень або інтерпретації невизначеності описів.

Для здійснення переходу від описів семантики, які мають наведеними вище особливостями, до формалізованого опису характеристик семантики аналізованих об'єктів необхідно вжити таких угоди:

— опис інтерпретаційних розширень об'єктів здійснювати в формалізованої формі;

— ввести певні вихідні умови заміни текстового опису семантики прийнятими числовими величинами на шкоду можливостей розширення або розширення якісних можливостей відповідних описів.

4.3. Аналіз способів формального опису інформаційних компонент систем управління доступом

Інтерпретаційні розширення, які використовуються для опису базових елементів системи, є основою для обчислення семантичних параметрів окремих елементів описів і фрагментів таких описів інформаційних компонент. У зв'язку з цим, одним з важливих вимог до складання словників предметної області є вимога до однозначності описів інтерпретаційних розширень і відповідно однозначності базових елементів. Це означає, що конструкції інтерпретаційних розширень повинні містити певну кількість елементів, в основному слів природної мови. Такі вимоги забезпечуються в першу чергу нормалізацією таких описів. Нормалізований опис відрізняється від ненормалізованого тим, що число синтаксичних правил побудови описів і безліч слів предметної області, істотно обмежена в порівнянні з різноманітністю синтаксичних правил і допустимих до використання слів, при формуванні подібного не нормалізованих описів. Такі скорочення стосуються різних неоднозначностей, синонімів і синтаксичних схем, які, з точки зору, надмірності, можуть бути заборонені до використання. Обмеження допустимих схем синтаксичних правил ґрунтується на визначенні обмеженої кількості класів слів, які визначаються на основі аналізу

загальноприйнятих значень відповідних слів, зокрема, в предметної області, яка описується відповідними розширеннями. До таких класів відносяться наступні типи слів, які прийняті до використання

— слова ідентифікатори об'єктів, процесів та інших базових елементів (клас B),

— слова ідентифікують перетворення елементів або їх стан (клас D),

— слова, які ідентифікують різні ознаки базових об'єктів У і слова класу D (клас H).

Зрозуміло, що клас B складають слова, які в граматиці природної мови є іменниками і т.д. Для складання фрагментів S_c, використовується ряд умов, які стосуються способів формування інтерпретаційних розширень.

Умова 4.4. Текстове представлення опису інтерпретаційного розширення j (X_i) має виконуватися тільки з використанням безлічі певних слів K, в якому всі слова однозначно розподілені на класи B, D і H.

Умова 4.5. Структури фрагментів $\varphi(j(X_i))$ повинні відповідати структурам, які визначаються синтаксичними правилами Ω.

Умова 4.6. Різні слова, які мають різну семантичну значимість, повинні описуватися різною кількістю слів в j (X_i).

Ця умова є одним з ключових положень, завдяки якому виникає можливість переходу від якісної характеристики семантики слова до визначення її кількісного значення.

Умова 4.7. При використанні в черговому j (X_i) слів зі словника S_c має зберігатися наступне співвідношення:

$$(j > i) \rightarrow [X_i \in j_k(X_i)].$$

Якщо ця умова має місце для конкретного X_j, то при обчисленні кількісних значень семантичних параметрів, j_k (X_j) розширюється шляхом доповнення j_k (X_j) описом $j_i(X_j)$. Ця процедура може бути рекуррентной, якщо $j_i(X_j)$ містить X_k задовольняють умові 4.3. або $(K < i)$.

Схеми синтаксичних правил описують допустимі послідовності класів слів, які можуть використовуватися при формуванні фрагментів описів або цілих пропозицій, які описують певну ситуацію в предметної області. Перш за все, правила Ω не повинні суперечити синтаксису граматики природної мови. Оскільки в результаті використання Ω, можуть бути побудовані два типи конструкції: фрази і пропозиції, то відповідні правила повинні орієнтуватися на побудови фраз і пропозицій φ. Очевидно, що за межами цих конструкцій, говорити про використання правил Ω, при побудові окремих описів не має сенсу. Оскільки синтаксичні правила використовуються на досить загальному рівні інтерпретації слів, на рівні класів або типів слів, то синтаксичні структури $\omega_i \in \Omega$ можна описувати на основі використання функцій математичної логіки $\{\vee,\&,\rightarrow,\neg\}$ [4]. Оскільки синтаксичні правила, в першу чергу, визначають структуру об'єктів, для побудови яких вони використовуються, то слід зазначити, що для природної мови європейських народів характерна послідовна структура фраз і пропозицій. Але це не означає, що не можна говорити і про інші структури текстового відображення φ або Ψ. Такі можливості, найчастіше використовуються у випадках, коли створюються тексти для спеціальних способів їх відображення, наприклад, для текстової реклами або для формування повідомлень на етикеткової продукції і т.д. В даному випадку, ми обмежимося строчечними структурами і відповідними їм системами синтаксичних правил. система Ω, в загальному випадку може бути записано у вигляді наступного співвідношення:

$$\Omega = F(\omega_i, ..., \omega_k),$$

де ω_i окрема структура φ або Ψ, F – функція, що описує взаємозв'язки між різними структурами. У найпростішому, функція F може являти собою функцію упорядкування ω_i за деякими ознаками, наприклад, за ознакою найбільш уживаною структури. Крім того, функція F відображає залежності між ω_i які орієнтовані на формування φ і ω_j, які орієнтовані на формування Ψ. Прикладом

таких співвідношень може служити співвідношення: $\omega_i(\varphi) \subset \omega_j(\Psi)$. Природно, що має місце співвідношення:

$$[\omega_j(\Psi_i) \not\subset \omega_i(\varphi_i)] \& [\omega_j(\Psi) = \omega_i(\varphi_i)] \to (\Psi = \varphi).$$

Оскільки поділ слів на класи не залежить від інтерпретації окремих слів в предметних областях, які описуються в S_c, то синтаксичні схеми є загальними для будь-яких предметних областей. Це не означає, що ті чи інші схеми $\omega_i \in \Omega$ можуть обумовлювати виникнення суперечностей, оскільки схеми Ω будуються відповідно до правил нормалізації довільних описів. Правила нормалізації описів, по суті, безпосередньо впливають на обрані синтаксичні схеми, оскільки нормалізація, як і синтаксичні схеми, є факторами, що обмежують допустимі способи опису фрагментів і пропозицій. Різниця між нормалізацією і синтаксичними схемами полягає в тому, що правила нормалізації використовуються для складання описів інтерпретаційних розширень $j_i(X_j)$, а синтаксичні схеми використовуються для формування текстових відображень фрагментів або пропозицій ψ, які будуються з $\{x_1, ..., x_n\} \subset S_c$. У загальному вигляді приклад окремої синтаксичної схеми представляється в такий спосіб:

$$\omega_i = (x_i \,\&\, x_j) \vee (x_k \,\&\, x_i) \to (x_m \,\&\, x_k).$$

Оскільки кожен ідентифікатор x_i у рамках S_c має своє текстове відображення, то фрагмент тексту, який побудований у відповідності зі схемою ω_i, може відображатися у вигляді сукупності слів природної мови. При цьому, логічні зв'язки замінюються описом їх інтерпретації на природній мові, наприклад $\& \Rightarrow \{u,\}$, $\vee \Rightarrow \{або\}$, $\Rightarrow = \{якщо \ldots то\}$. Використання логічного оператора заперечення $\neg$, вимагає більш детального розгляду. Одномісна функція заперечення означає що змінна має значення протилежне значенню змінної, яке в даному випадку, допускає інтерпретацію наявності відповідного слова в φ або Ψ. Тоді його заперечення може означати неприпустимість вживання відповідного слова φ або Ψ, що можна інтерпретувати, як його виключення з $(\varphi \vee \Psi)$. Тоді необхідність в операторі може виявитися надмірною. Насправді, синтаксичні схеми допускають

структури, в яких описуються альтернативні стани або умови функціонування діючих суб'єктів в системі BSD. Тому у відповідному описі необхідно використовувати оператор заперечення.

Основна мета використання семантичних параметрів полягає в тому, щоб перейти від якісного аналізу семантики до кількісного її аналізу. Такий перехід можливий лише за таких умов:

— при формуванні обмежень на допустиме розширення інтерпретації окремих елементів;

— при введенні умов визначення масштабу вимірювання кожного з розглянутих параметрів;

— при визначенні способів взаємозв'язку між окремими семантичними параметрами, які дозволили б обчислювати числові, логічні та інші значення одних параметрів на основі значень інших параметрів.

Природня мова, за своєю природою є системою досить гнучкою, що забезпечується можливістю розширення семантичної інтерпретації окремих елементів. Це властивість проявляється в існуванні слів, як окремих елементів мови, які можуть мати досить різні семантичні значення. Це ж властивість мови проявляється в наявності досить великої кількості синонімів, яка присутня у всіх мовах і ця множина тим більше, ніж менш аналітична та чи інша природня мова.

Способи визначення величини числового значення того чи іншого параметра є найбільш критичними, з точки зору теорії лінгвістики [5]. Це обумовлюється необхідністю прийняття нових угод в різних аспектах значень окремих слів, що не відповідає базовим підходам в дослідженні семантики в лінгвістиці. Тому наведені обмеження в даній роботі носять робочий характер і пов'язані тільки з проблемами, які в даному випадку досліджуються.

Необхідність існування конструктивних взаємозв'язків між окремими семантичними параметрами ґрунтується на доцільності формування коштів семантичного аналізу інформаційних компонентів, як засобів, які становлять єдину систему семантики інформаційного забезпечення SRD.

Введемо наступні семантичні параметри, які будуть характеризувати семантику інформаційних засобів системи BSD, які допускають текстове відображення на природній мові:

— семантична значимість елемента (z);

— семантична ефективність елемента (e);

— противоречивость фрагмента (h);

— узгодженість фрагментів в реченні (u);

— рівень конфліктності пропозицій (k).

Розглянемо способи визначення їх числових значень, для чого розглянемо такі визначення.

Визначення 4.1. Величина семантичної значимості елемента визначається числом інформаційних компонент, які використовуються для опису інтерпретаційних розширень відповідних елементів x_i.

Формально $z(x_i)$ можна записати у вигляді наступного співвідношення: $z(x_j) = \sum_{i=1}^{n} Sg(a_i)$. Виходячи з визначення $z(x_i)$, можна було б записати, що $z(x_i) = k$, де $i = (1, ..., k)$, але в процесі використання S_c і відповідних $j(x_i)$, інтерпретаційні розширення можуть модифікуватися. Така модифікація може складатися в додаванні в $j(x_i)$ нових компонент a_i або у видаленні використовуваних компонент a_i з $j(x_i)$. В останньому випадку, замість віддаленої компоненти в $j(x_i)$ на відповідне місце вписується нуль. Необхідність в проведенні відповідних модифікацій обумовлюється умовами обмеження семантичної інтерпретації відповідних елементів на етапі вихідного формування інформаційних компонент і, в першу чергу, словника S_c.

Визначення 4.2. Величина семантичної ефективності елементів x_i визначається частотою використання відповідних елементів в алгоритмах рішення прикладних задач.

Цей параметр і, відповідно, його величина записується у вигляді технічного доповнення інтерпретаційного опису $j(x_i)$. При розширенні асортименту

семантичних параметрів, кількість таких технічних доповнень може зростати. Поточне значення параметрів, які описуються в технічних додатках $j(x_i)$ в процесі використання x_i змінюються. В цьому випадку $j(x_i)$ запишеться у вигляді

$$j(x_i) = \{< a_1, ..., a_n > | ... | < a_1, ..., a_k > | [e = m]\}.$$

Визначення 4.3. Суперечливість фрагментів $h(\varphi_i)$ визначається функцією *f* семантичних параметрів слів з *z* і *E*, які використовуються для формування відповідного фрагмента.

Формально, цей параметр можна описати співвідношенням: $h(\varphi_i) = f(z, e)$. В процесі розвитку інформаційних засобів вид функції *f* може змінюватися. Тому, приймемо перше наближення способу побудови функції *f*. Перш за все, приймемо, що в початковому стані *e* не змінюється і дорівнює нулю. Тоді можна записати, що $h(\varphi_i) = f_1(z)$. Оскільки φ_i в текстовій формі мають лінійну структуру, що відповідає прийнятій формі написання текстів, то введемо змінну r, яка відображає номер поточного слова в φ_i. Тоді можна записати, що

$$h(\varphi_i) = f_1(z, r).$$

В цьому випадку, можна говорити про різниці між значеннями z_i і z_j для слів з номерами *i* і *j*. Оскільки φ_i передбачає задану послідовність слів x_i тоді $\Delta z_i = |z(x_i) - z(x_{i-1})|$. В цьому випадку, можна говорити про те, що семантична суперечливість може змінюватися в деякому діапазоні числових значення. Приймемо, що семантична суперечливість виникає в разі, якщо $\Delta z_i \geq z_{\max}$, де $z_{\max}$ вибирається апріорі. Природньо припускати, що $\varphi_i(x_1, ..., x_i)$ може мати різний рівень суперечливості і, при цьому може зберігати допустиму в системі інтерпретацію. У цьому полягає принципова відмінність семантичної суперечливості від логічної суперечливості [6], яка визначається однозначно. Формально, перший варіант функції f_1 може бути представлений таким чином:

$$h(\varphi_i) = (m = 0) \,\&\, \{\textstyle\sum_{i=1}^{n} [|z_{i+1} - z_i| - \Delta z_{\max}] \rightarrow (m = m + 1) \,\&\, [h_i(z_{i+1}, z_i) = \\ = |z_{i+1} - z_i| - \Delta z_{\max}]\} / m,$$

де m – кількість пар слів, для яких різниця в семантичної значущості перевищило $\Delta z_{\max}$, $h_i(z_{i+1}, z_i)$ – елементарна семантична суперечливість двох слів z_{i+1} та z_i. Параметр, який описує узгодженість двох пропозицій, що відносяться до однієї проблеми, описує семантичний взаємозв'язок між пропозиціями в межах фрагмента тексту, що містить опис обраної прикладної задачі. Цей параметр можна розглядати, як аналогію суперечливості фрагмента φ_i, визначення якої наведено вище. Оскільки величина суперечливості, яка приймається допустимої для φ_i змінюється в деякому інтервалі $[\alpha, \beta]$, який визначається апріорно, то і величина узгодженості фрагментів в інтервалі теж може змінюватися в деякому інтервалі. У загальному випадку приймемо, що величина суперечливості $h(\varphi_i)$ обмежена тільки знизу, тобто виразно, для $h(\varphi_i)$ значення $\Delta z_{\max}$, яке визначає факт виникнення суперечливості. Аналогічно приймемо і для параметра u максимально допустиме значення $h(\varphi_i)_{\max}$, після якого визначається факт існування неузгодженості між фрагментами φ_i і φ_j, які складають пропозицію. Розглянемо наступне визначення.

Визначення 4.4. Міра неузгодженості $u(\varphi_1, ..., \varphi_m)$ між фрагментами пропозиції Ψ визначається на основі максимальних значень величин суперечливості в кожному з фрагментів φ_i.

Формально, цей параметр описується співвідношенням:

$$u(\Psi_i) = [\sum_{i=1}^{m} h(\varphi_i)] / m,$$

де m – кількість текстових фрагментів φ_i в реченні Ψ_i. У цьому співвідношенні до уваги береться ситуація, коли міра суперечливості окремої пари фрагментів φ_i і φ_j имеет локальный максимум и существенно отличается от мер противоречивости остальных фрагментов, что может существенно влиять на решение прикладных задач. Необходимо отметить, что в данном случае, под фрагментом φ_i пропозиції Ψ_i мається на увазі окрема фраза. Кожна фраза, в першу чергу її мінімальний розмір, визначається окремою синтаксичної схемою $\omega_i \in \Omega$.

Параметр потенційної конфліктності пропозицій, як і параметр $u(\Psi_i)$ визначається на основі попередніх семантичних параметрів, в даному випадку, на основі параметра $u(\varphi_i)$. Параметр $K(\Psi_i)$ визначає семантичний зв'язок між окремими пропозиціями і позначається $K(\varphi_i, \Psi_i)$. Цей параметр є більш складним, ніж параметр $u(\varphi_i, \varphi_j)$, оскільки при його визначенні можуть використовуватися не тільки послідовно розміщені пропозиції Ψ_i і Ψ_{i+1}, але і пропозиції, які розділені іншими пропозиціями. В даному випадку обмежимося розглядом двох послідовних пропозицій.

Визначення 4.5. Потенційна конфліктність $K(\Psi_i, \Psi_{i+1})$ між двома послідовними пропозиціями дорівнює абсолютному значенню різниці заходів їх неузгодженості.

Формально $K(\Psi_i, \Psi_{i+1})$ визначається співвідношенням:

$$K(\Psi_i, \Psi_{i+1}) = \left| u(\Psi_i) - u(\Psi_{i+1}) \right|.$$

Розглянемо коротко інтерпретацію зміни величин семантичних параметрів з точки зору зміни можливих значень семантики текстових відображень інформаційних компонент.

Ототожнення семантичної значущості з кількістю інформаційних компонент, які описують один елемент x_i, грунтується на наступних положеннях. Першим з них є вимоги складати текстові описи окремих елементів в нормалізованій формі. Це означає, що $j(x_i)$ буде містити таку кількість слів, в середовищі яких не буде надлишкових слів і не буде слів, які допускають для даного випадку їх вживання, неоднозначності в позначенні тих параметрів або особливостей, для опису яких вони вживаються. Якщо можливості природної мови, яка використовується для складання описів $j(x_i)$, не дозволяють забезпечити таку можливість, то в словнику S_c формується система приміток, в якій описуються відповідні обмеження у визначенні значень відповідних слів. Форма опису приміток відповідає формальним засобам системи аналізу семантичних параметрів, які здійснюють визначення та перетворення семантичних параметрів.

Друге положення, як і перше, відносяться до процесу формування опису $j(x_i)$. Всі описи $j(x_i)$ формуються відповідно до системи синтаксичних схем, які обмежують, з точки зору можливостей природної мови, способи формування текстових описів $j(x_i)$. Такі обмеження формуються на основі врахування особливостей предметної області, для якої складаються відповідні системи синтаксичних схем.

Наступне положення полягає в відображенні особливостей використання S_c в процесі функціонування системи, що використовує інформаційні засоби. Ці особливості описуються у вигляді технологічних доповнень і їх величина може визначати значення відповідного семантичного параметра. В даному випадку, відповідним семантичним параметром є семантична ефективність.

Наведені вище семантичні параметри, відповідно до їх визначень, можна розглядати як деяку ієрархічну систему. Ієрархія, в даному випадку розглядається як деяке семантичне узагальнення поточних параметрів попередніх в такий ієрархії параметрів. Формально, таку ієрархічну залежність між параметрами опишемо наступним співвідношенням:

$$K(\Psi_i, \Psi_j) \to u(\Psi_i) \to h(\varphi_i) \to e(x_i) \to z(x_i). \qquad (4.4)$$

З точки зору семантичної інтерпретації, це співвідношення відображає наступні обставини:

— кожна посилка є семантичним узагальненням наслідків, які за нею йдуть;

— кожна посилка допускає більш широку семантичну інтерпретацію, по відношенню до наступних посилок, при цьому, розширення такої інтерпретації не визначається однозначно інтерпретаціями відповідних наслідків;

— неоднозначність розширення інтерпретації посилки в залежності від слідства.

З визначень $K(\Psi_i, \Psi_{i+1})$, $u(\Psi_i)$, $h(\varphi_i)$ випливає, що кожна посилка може розглядатися, як наслідок або узагальнення попереднього в (4.4.) семантичного параметра. Формальний опис кожного з параметрів передбачає певний спосіб обчислення величини відповідного параметра. Особливе місце в (4.4) займають

параметри $z(x_i)$ і $e(x_i)$. Тому, будемо їх називати атомарними або первинними семантичними параметрами. Решта семантичні параметри будемо називати похідними параметрами. Очевидно, що кількість базових параметрів може бути розширено, оскільки, останні можуть бути пов'язані з особливостями функціонування системи, яка використовує відповідні параметри, наприклад, параметр $e(x_i)$. Розширення базових семантичних параметрів вимагає використання зворотних зв'язків між подіями в системі і, в першу чергу, між інформаційними компонентами S_c. Наприклад, нехай використання x_i найбільш часто призводить до збільшення $h[\varphi_i(..., x_i)]$, тоді можна ввести атомарний семантичний параметр і заходи семантичної критичності x_i і т.п.

4.4. Дослідження взаємозв'язків між семантичними параметрами для систем розмежування доступу

Необхідність дослідження взаємозв'язків між семантичними параметрами обумовлюється наступними факторами та особливостями цих параметрів:

— існуванням взаємозалежностей між параметрами, які описуються в їх визначеннях;

— необхідністю семантичної інтерпретації різних значень величини цих параметрів;

— існуванням критичних значень величин семантичних параметрів, обмеженими діапазонами їх значень і особливими точками значень відповідних параметрів.

Введення чисельних значень семантичних параметрів має сенс, якщо семантичною інтерпретацією володіють не тільки самі параметри, але і окремі величини їх значень. Встановлення такої інтерпретації можна здійснювати наступними способами:

— на основі апріорних методів формування інтерпретації різних значень семантичних параметрів;

— на основі дослідження зміни значень параметрів, які визначаються із взаємозв'язків між параметрами;

— на основі експериментальних досліджень фрагментів предметної області і змін в текстових описах в цілому, при зміні значень окремих параметрів;

— на основі об'єктивних обмежень, які накладаються на діапазони значень параметрів, виходячи з аналізу специфіки предметної області.

Останній спосіб визначення семантичної інтерпретації значень параметрів, в першу чергу, використовується по відношенню до базових семантичним параметрами, до яких відносяться:

— семантична значимість $z(x_i)$;

— семантична ефективність $e(x_i)$ та інші базові параметри, які можуть вводитися при необхідності.

Розглянемо більш детально цей спосіб введення обмежень на величини значень семантичних параметрів на якісному рівні. Нехай деяка компонента x_i із $j(x_i)$ володіє інтерпретаційним розширеням $j(x_i)$, котре складається із m інформаційних елементів, що формально описується співвідношенням $j(x_i) =< a_1, ..., a_m >$. В цьому випадку величини семантичної значущості x_i определяются соотношением: $z(x_i) = \sum_{i=1}^{n} Sg(a_i)$.

$z(x_i) = \sum_{i=1}^{n} Sg(a_i)$. Для реалізації способу інтерпретації значень поточних величин базових семантичних параметрів, скористаємося поняттям рівня абстракції компонентів x_i словника S_c, котре вже розглядалося раніше. При розгляді поняття рівня абстракції використовуються два функціональних перетворення:

— $F_{Ai}(S_{ci})$ – перетворення окремих елементів з S_c яке призводить до зміни рівня абстракції груп із S_c;

— Q_{Ai} – функція, відповідно до якої визначається величина зміни рівня абстракції.

У загальному випадку, збільшення рівня абстракції деякого підмножини $\{x_{i1}, ..., x_{im}\} \subset X$ має семантичну інтерпретацію, яка може, на якісному рівні характеризуватися такими особливостями:

— збільшення рівня абстракції позначення окремих елементів S_c доцільно в тому випадку, якщо нові елементи x_j^* мають більш загальне значення по відношенню до x_i;

— використання x_j^* для створення φ_j^* дозволяє формувати фрагменти, які описують відповідні фрагменти предметної області без урахування окремих деталей, які носять приватний характер і не потрібні для встановлення більш загальних, для даної предметної області, описів;

— оскільки збільшення рівня абстракції, в даному випадку, зв'язується з можливістю формування більш загальних описів процесів або компонент, які присутні в предметної області, то використання різних рівнів абстракції дозволяє будувати алгоритми реалізації окремих процесів таким чином, щоб рішення задачі, на яку орієнтований відповідний процес, можна було досягти більш ефективним способом;

— в загальному випадку, можна стверджувати, що використання об'єктів більш високого рівня абстракції для опису процесів, в яких вони беруть участь у багатьох випадках, дозволяє отримати рішення відповідний завдання в більш загальному вигляді.

Розглянемо більш детально, що являє собой функція $F_{Ai}(S_{ci})$, в рамках розглянутого підходу. Оскільки F_{Ai} здійснює перетворення фрагмента $S_{ci} \subset S_c$,то для спрощення розгляду, обмежимося одним елементом x_i. Для опису $j(x_i)$ використовуются компоненти $\{a_1, ..., a_n\}$,які в предметній областіW являються словами природної мови V. Елементи x_i із S_c повинні представляти собой слова, які для предметної області W теж відносяться до відповідного природної мови V, оскільки фрази і пропозиції, які формуються в рамках інформаційних засобів, орієнтовані на використання користувачами системи доступу. Очевидно, що в

рамках самої системи відповідні елементи позначаються ідентифікаторами. Якщо $\{x_1, ..., x_m\} \cup \{a_1, ..., a_n\} = v$, то v є множиною слів для V, які описує W. Для зручності V і W. будемо ототожнювати, оскільки предметна область реалізується за допомогою описів на відповідному природною мовою.

Для формування φ_i і Ψ_i використовується, окрім семантичних правил і обмежень, синтаксичні схеми $\Omega = \{\omega_1, ..., \omega_2\}$. Оскільки v являється загальним для x_i і для $j(x_i)$, то можно прийняти, що в $j(x_i)$ окремі фраз из $a_{i1}, ..., a_{im}$ формуються також в співвідношенні з правилами Ω, тим більш, що и для створення опису $j(x_i)$ і опису $\varphi_i(x_{i1}, ..., x_{ik})$ використовуються однакові вимоги щодо нормалізації відповідних текстових відображень. Отже, можна записати, що V або W: являє собою мову, який описується наступним співвідношенням:

$$W = (v, \Omega, X_i^B),$$

де X_i^B – набір елементів S_c найбільш низкого рівня абстракції.

Функція $F_{Ai}(x_i)$, $F_{Ai}(x_i)$, По суті, є породжує функцією, оскільки базовий елемент X_i^B не може бути переведеним на вищий рівень абстракції,оскільки X_i^B має певну $j(X_i^B)$, яка сформована в вихідному випадку. Тому, правильніше було б функцію породження представити в наступному вигляді:

$$X_i^m = F_{Ai}(X_{i1}^{m-1}, ..., X_{ik}^{m-1}), \qquad (4.5)$$

де X_i^m – елемент S_c з рівнем абстракції m, X_{ij}^{m-1} – елемент S_c з рівнем абстракції $m-1$. Співвідношення (4.5) описує породження суворої ієрархії, коли рівень абстракції m формується основі попереднього рівня абстракції $m-1$. Частіше всього функція F_{Ai} реалізує перетворення вільної ієрархії. Це означає, що має місце співвідношення:

$$X_i^m = F_{Ai}(X_{i1}^{m-1}, ..., X_{ik}^{m-1}, ..., X_{im}^B),$$

де елемент X_i^m породжується не тільки на основі елементів попереднього рівня абстракції, а й на основі перетворення елементів різних нижчих рівнів ієрархії, включаючи і базовий рівень X_{im}^B. Для спрощення розгляду приймемо, що:

$$X_i^2 = F_{A1}(X_{i1}^B, ..., X_{ik}^B) \text{ или } X_i^2 = F_{A1}(X_j^B).$$

В цьому випадку , F_{Ai} буде здійснюватися перетворення $j(x_i)$ таким чином, щоб в множині $\{a_{i1}, ..., a_{im}\}$ зявився хоча б один елемент із X_j^B і відповідно з S_c. Формально це можна записати в такий спосіб:

$$X_j^2 = F_{A1}(X_j^B) = F_{A1}(< a_{j1}, ..., a_{jm} >) =< a_{j1}, ..., x_i^B, ..., a_{jm} >$$

Природничо ,що $x_i^B =< a_{i1}, ..., a_{ik} >,$ тоді можна записати:

Наведені перетворення не означають, що за допомогою F_{Ai} в W можна породити фізично новий елемент елементами поточного рівня абстракції , як правило, є нові поняття про W, нові процеси, які можуть виникати в W, і в крайньому випадку, нові фізичні об'єкти, якщо в рамках системи, яка використовує відповідну інформаційну компоненту можливо фізичне виготовлення нового фізичного елементу x_i^m.

Співвідношення (4.6), яке описує новий елемент S_c з новим рівнем абстракції, в силу вищого рівня абстракції x_i^m має семантичну значимість відмінну від семантичної значущості елемента x_i. $j(x_j)$ Цей факт забезпечується в даному випадку, додаванням в інтерпретаційного розширення $j(x_i)$. Таке додавання здійснюється відповідно до правил Ω. Таким чином , функція F_{Ai}, по суті, вибирає додаткові елементи $x_{i1}, ..., x_{ik}$, із S_c і розширює ними $j(x_j)$. Отже, можна прийняти, що збільшення семантичної значущості $z(x_i)$ в визначається величиною, яка визначається кількістю інформаційних компонент в $j(x_i)$. Процес вибору компонент, якими передбачається розширювати $j(x_i)$ не може бути довільним. Це означає, що функція $F_{Ai}(x_i)$ повинна визначатися більш конструктивно. Перш за все, на процес вибору впливають синтаксичні схеми, відповідно до яких побудовано розширення $j(x_i)$. На підставі $\omega_i(x_i)$ визначається місце розміщення розширювача $j(x_j)$ в $j(x_i)$. В більшості випадків, таке розширення реалізується в кінці опису $< a_{i1}, ..., a_{im} >$, якщо параметри суперечливості та узгодженості фрагмента $j[\varphi_i(a_{ij})]$ у існуючого $j(X_i)$

задовольняють заданим вимогам оскільки мова W один для $j(X_i)$ і для $A_i(X_i)$, то семантичні параметри, які введені для текстових описів прикладної системи $A = \{A_1, ..., A_m\}$, використовуються і для аналізу текстових описів інтерпретації $J(A_i)$. Для їх розрізнення, в останньому випадку, відповідні позначення будемо писати у вигляді того ж символу з індексом j зверху, або z^j, e^j, h^j, і u^j. Приймем, що $j(X_i)$ можуть являти собою фрази φ^j або речення Ψ^j, тому параметр $k(\Psi_i, \Psi_j)$ для $J(A)$ не розглядається. Наступним обмеженням, яке уточнює спосіб реалізації $F_{Ai}(X_i)$, є задані допустимі значення величини зміни семантичних параметрів z^j, e^j, h^j, і u^j. Такі значення є загальними для всієї предметної області W_i. Відзначимо, що в рамках S_c. предметних областей може бути кілька, наприклад, в разі використання в рамках BSD різних методів ідентифікації.

Функція Q_{Ai} відрізняється F_{Ai} тим, що вона визначає міру зміни рівня абстракції перетвореного фрагмента S_{ci} в словнику S_c. Як мінімум, вона повинна враховувати умову 4.3, хоча, в загальному випадку, ця функція може визначатися більш складним способом, який враховує більш широко параметри прикладної системи, наприклад, рівень безпеки системи доступу або рівень ризику роботи користувача з об'єктом доступу, який оснащений відповідною системою доступу.

З викладеного вище видно, що функція F_{Ai} відповідає класичному уявленню про аналітичні функції [7]. Ця функція являє собою систему умов і окремих алгоритмів вибору і алгоритмів аналізу семантичних параметрів в $J(A)$.

Розглянемо обмеження на діапазон значень параметра $Z_i(x_i)$. Оскільки $j(x_i)$ має являти собою фразу, то система синтаксичних правил визначає мінімально допустима кількість слів, яке необхідно для того, щоб фраза була сформована синтаксично коректно. В даному випадку приймемо, що мінімальна за розміром фраза повинна складатися, як мінімум з трьох слів. Ця умова передбачається в конкретних схемах $\omega \in \Omega$. Для визначення верхньої межі кількості допустимих

слів в межах фрази φ^j введемо додатковий семантичний параметр, який описується наступним визначенням.

Визначення 4.6. Семантична надмірність фрази $\eta(\varphi_i)$ визначається похідною від функції $f(z_i)$, яка визначена на φ_i, по змінної збігається з віссю розташування слів у фразі φ_i.

Формально це можна записати у вигляді:

$$\eta(\varphi_i) = df(z_i)/d_i,$$

де $f(z_i)$ крива, яка апроксимує величини значень z_i для кожного з послідовно розміщених в фразі φ_i слів x_i, i – номер слова в φ_i, починаючи від початку фрази і закінчуючи останнім словом фрази. Цю похідну можна замінити для дискретного випадку, кутом нахилу лінії зв'язує дві сусідні точки значень семантичної значущості двох послідовних слів x_i і x_j в фразі φ_i, Середнє значення відповідних кутів по всій фрази φ_i буде характеризувати міру семантичної надмірність $\eta(\varphi_i)$. Слід зазначити, що, для визначення семантичної надмірності, кут нахилу вибирається між гіпотенузою і вертикальною віссю, оскільки елементарний прямокутний трикутник будується паралельно вертикальної і горизонтальної осі z і i. Формально, це запишеться у вигляді співвідношення:

$$\eta(\varphi_i) = \{\sum_{i=1}^{m-1} \text{arctg}\,[(|z_j^i - z_{i-1}^k|)/(i_i^j - i_{i+1}^k)]\}/(m-1), \qquad (4.7)$$

де i_j – номер чергового слова у фразі φ_i.

Розглянемо якісну інтерпретацію цього параметра. Нехай деякі два послідовних слова x_i і x_j в фразі φ_i. мають однакову семантичної значимістю. При цьому, можна припустити, що семантична значимість визначається не одним, а поруч базових семантичних параметрів.

В такому, випадку $z(x_i) \approx z(x_j)$, то два слова x_i і x_j. є синонімами і їх спільне вживання суперечить вимогам нормалізованого уявлення текстових відображень. У співвідношенні (4.7) в знаменнику, якщо розглядати два послідовних слова знаходиться одиниця, оскільки масштаб горизонтальної осі визначається

кількістю слів на заданому відрізку цієї осі. Тому, відстань між двома суміжними словами завжди дорівнює одиниці або вимірюється кількістю слів в, а якщо йдеться про відстань між не суміжними словами.

Відповідно до вимог використання нормалізованих методів побудови текстових образів, система Ω передбачає певні обмеження на допустимий розмір фраз φ_i і відповідно, на допустимий розмір пропозицій Ψ, які можуть використовуватися в прикладній системі A_i. Проте, в межах допустимих розмірів фраз можуть виникати семантичні надмірності внаслідок використання семантично близьких слів. Щоб допустима довжина фраз обмежувалася не тільки синтаксичними схемами але і семантичними чинниками, необхідно для кожної φ_i визначати величину $\eta(\varphi_i)$. Якщо $\eta(\varphi_i) < \eta(\varphi_i)_{\min}$, то розмір відносно φ_i не допустимий. Таким чином верхня межа допустимого розміру фрази φ_i в A_i і $J(x)$, є плаваючою і може бути різною, для різних φ_i.

Розглянемо діапазон допустимих значень для параметра $e(x_i)$.У вихідному випадку $e(x_i)$ має фіксоване початкове значення, що визначає для кожного $e(x_i)$ його мінімальну межу в діапазоні значень цього параметра. У рамках даного підходу розглядається ситуація, коли φ і Ψ із A_i формуються при проектуванні прикладної системи A_i. Такі фрази і пропозиції становлять базову систему текстового відображення прикладної системи A_i.. Це не означає, що вся A_i повинна бути описана в текстовому вигляді. Текстовому відображенню підлягають тільки ті фрагменти, які не можуть бути описані в рамках формальних засобів, які використовуються для проектування відповідної прикладної системи. A_i.Прикладом такої ситуації, характерної для області захисту даних і, зокрема, для систем розмежування доступу, є BAN-логіка [8]. На підставі аналізу використовуваних інформаційних елементів X_i з S_c позначити S_t, в базовій системі фраз і пропозицій, яке будемо позначати, визначається початкове значення параметра $e(x_i)$ і на момент проектування A_i відповідне значення $e(x_i)$ для окремого $e(x_i)$ приймається в якості граничного. Встановлення діапазону

значень $e(x_i)$ для S_c в частині нижньої його межі здійснюється відповідно до співвідношення.

$$\min[gr(e(x_i))] = \min(e(x_i))^B,$$

де $e(x_i)^B$ - мінімальне значення $e(x_i)$ встановлене на основі аналізу базових φ_i і Ψ_i з S_t. Максимальне значення в даному разі, не будемо вводити в якості обмеження діапазону значень, оскільки, це вимагає більш глибокого аналізу семантики всієї предметної області в цілому на кожному етапі її розвитку. Відзначимо лише, що в рамках даного дослідження, що не передбачається реалізація можливості формування в автоматичному режимі, в процесі функціонування системи нових фраз або пропозицій Ψ,а використання інформаційних засобів дозволяє тільки модифікувати φ_i і Ψ_i, які знаходяться S_t. Природно, що процес послідовних модифікацій, який реалізується на різних етапах функціонування системи може привести до появи нових φ_i і Ψ_i, які не відповідають φ_i^B і Ψ_i^B.

Розглянемо допустимі діапазони значень для параметра $h(\varphi_i)$. Семантична суперечливість в рамках однієї фрази φ_i избыточности є альтернативним поняттям для семантичної надмірності $\eta(\varphi_i)$. Як і в разі $\eta(\varphi_i)$, для семантично повного визначення $h(\varphi_i)$ може виникнути необхідність у більш широкий асортимент базових семантичних параметрів, ніж параметри $z(x_i)$ і $e(x_i)$.Оскільки, в даному випадку, ми обмежуємося базовим параметром $z(x_i)$, то межі значень параметрів $h(\varphi_i)$ Мінімальне значення встановлюються таким чином. $h(\varphi_i)$ переходить в міру параметра $\eta(\varphi_i)$ і відповідає мінімально допустимій величині параметра $\eta(\varphi_i)$. Таким чином можно записати

$$\min[gr(h(\varphi_i))] = \min(\eta(\varphi_i))],$$

де $gr(y)$ означає граничне значення аргументу *y*. Максимальне значення діапазону допустимих значень для параметра $h(\varphi_i)$ визначається, для випадку двох суміжних слів співвідношенням::

$$\max[gr(h(x_i, x_j)] = \max[gr[z(x_i)] - 3].$$

Цей випадок відповідає ситуації, коли слово x_i має максимальне значення *z*, визначається граничною величиною, а слово x_j має максимальне значення *z*, яке, відповідно до прийнятого вище, так само трьом інформаційним компонентам в $j(x_j)$. Оскільки верхня межа значень параметра $z(x_i)$ істотно залежить від семантики предметної області W і від семантичної інтерпретації процесів, які відбуваються в W під час функціонування відповідної прикладной системи A_i, то максимально допустимі граничні значення для $\eta(\varphi_i)$ встановлюються на основі даних отриманих в результаті експлуатації відповідної прикладної системи A_i в *W*. Кінцевими критеріями, які використовуються в даному випадку, для визначення $gr(h(\varphi_i))$,є критерії рівня безпеки системи BSD, яка представляє собою предмет досліджень.

Граничні значення діапазону допустимих величин визначаються на основі аналізу граничних значень для $h(\varphi_i)$, оскільки $u(\varphi_1, ..., \varphi_n) = u(\Psi)$ визначається через $h_1(\varphi_i), ..., h_n(\varphi_n)$.Тому, більш детально розглядати це питання не будемо.

Діапазон значень параметра $K(\Psi_i, \Psi_j)$ для випадку суміжних пропозицій Ψ_i і Ψ_{i+1} розглядати не будемо, оскільки, цей випадок, аналогічний ситуації з параметром $h(\Psi_i)$. Складніша ситуація з визначенням діапазонів значень для $K(\Psi_i, \Psi_j)$ обумовлюються тим, що між Ψ_i і Ψ_j можуть розташовуватися інші пропозиції. Параметр K для цього випадку будемо позначати символом $K_R(\Psi_i, \Psi_j)$. Очевидно, що один із способів визначення величини $K_R(\Psi_i, \Psi_j)$ в вигляді.і відповідно, визначення діапазонів значень для може складатися в зведенні до послідовності K, що формально записується у вигляді

$$K_R(\Psi_i, \Psi_j) = F[K(\Psi_i, \Psi_{i+1}), ..., K(\Psi_{j-1}, \Psi_j)]$$

Можливість реалізації такої редукції грунтується на тому, що текстове відображення в довільний момент процесу функціонування являє собою деякий єдиний. Є певний єдиний текст, який описує в W. У цьому випадку, предметом обговорень може бути тільки функція F. Оскільки, в охоплюється цілий фрагмент зокрема відображення, то природно припустити, що в такому фрагменті відображаються глобальні для системи захисту доступу параметри. У зв'язку з цим конструктивний розгляд можливо в рамках розгляду BSD в цілому або в рамках окремих режимів функціонування BSD.

З викладеного вище, особливо, в частині що стосується встановлення граничних значень параметрів $z(x_i)$, $h(\varphi_i)$ а також $K_R(\Psi_i, \Psi_j)$ видно, що для вирішення задач встановлення допустимих значень параметрів, а також для встановлення більш повних взаємозв'язків між семантичними параметрами, необхідно використовувати підходи, в яких досліджується робота системи BSD в цілому, що пов'язано з експериментальними дослідженнями.

4.5. Висновки до четвертого розділу

У четвертому розділі розроблені базові інформаційні компоненти для розширення засобів захисту системи доступу з метою використання опису складових частин системи захисту на природному мовою. Для цього проаналізовано основні інформаційні компоненти. Показані і формалізовані семантичні умови існування таких компонент. Запропоновано схему засобів системи розмежування доступу і проведено дослідження взаємозв'язків між семантичними параметрами для розширення функціональних можливостей при здійсненні контролю доступу.

Список використаних джерел до четвертого розділу

1. K. Chen, «A new identification algorithm», *E. Dowson, J. Golic, eds. Cryptography: Policy and Algorithms. Lecture Notes in Computer Science*, vol. 1029, pp. 244-249, 1995.

2. U. Feige, A. Fiat, A. Shamir, «Zero-knowledge proofs of identity», *Journal of Cryptology*, vol. 1, no. 2, pp. 77-94, 1988.

3. Дж. Мак-Кинси, *Введение в теорию игр*, М.: ФМЛ, 1960, С. 420.

4. П. С. Новиков, *Элементы математической логики*, М.: Наука, 1973, С. 399.

5. В. А. Минаев, И. В. Пеньшин, В. Е. Потанин, С. В. Скрыль, «Аналіз загроз безпеки інформації в інформаційно-телекомунікаційних системах», [Електронний ресурс], *Я-Охоронець*, Режим доступу: http://www.bodyguard.ru.

6. Э. Мендельсон, *Введение в математическую логику*, М.: Наука, 1971, С. 320.

7. И.Н. Бронштейн, К.А. Семендяев, *Справочник по математике для инженеров и учащихся вузов. Изд. 13-е, испр.*, М.: Наука, 1986, С. 544.

8. N. Heintze, J.D. Tygar, «A Model for Secure Protocols and their Compositions», *1994 IEEE Symposium on Security and Privacy*, pp. 2-13, 1994.

РОЗДІЛ 5. МЕТОДИ АДАПТАЦІЇ ЗАСОБІВ ЗАХИСТУ СИСТЕМ РОЗМЕЖУВАННЯ ДОСТУПУ

5.1. Основні способи реалізації процесів адаптації при вирішенні завдань захисту систем доступу

Проблема адаптації в своєму абстрактному формулюванні є досить загальною, тому вона може розглядатися з точки зору різних аспектів своєї прояви. З цієї ж причини вона досить тісно пов'язана з широким класом близьких понять, таких як навчання, самоорганізація, з поняттями розвитку різного типу. У зв'язку з цим, розглянемо основні відмінності процесу адаптації від інших близьких за характером процесів. Перш за все, розглянемо відмінність між адаптацією та навчанням з точки зору їх принципових положень.

Навчання на найзагальнішому рівні характеризується наступними факторами:

— навчання передбачає наявність попередньо сформованої мети, яка повинна бути досягнута в результаті реалізації процесу навчання;

— навчання передбачає використання певних вихідних даних, які будуть використовуватися при реалізації процесу навчання;

— процес навчання може оцінюватися на основі аналізу досягнення мети, яка сформульована попередньо;

— процес навчання має певний інтервал своєї реалізації по відношенню до студента об'єкту.

Другим, родинним процесу адаптації, є процес самоорганізації. Основними факторами, які визначають цей процес, є:

— наявність критеріїв оцінки можливостей системи, як об'єкта реалізує один або кілька процесів, завдяки яким можна було б зміни в об'єкті, що представляють собою самоорганізацію, розпізнавати як такі, які призводять до позитивних змін, здатною піддатися кількісній оцінці;

— величина змін параметрів, за якими оцінюється і розпізнається процес самоорганізації, є позитивною, це означає, що відомо напрямок змін значень відповідних параметрів;

— процес самоорганізації відбувається за рахунок факторів, які визначаються самою системою, що передбачає неминучість існування в рамках самої системи спеціальних засобів, які можуть реалізовувати процеси самоорганізації;

— процеси самоорганізації, як і процеси навчання, відбуваються в виділені періоди часу і ці процеси не можуть суміщатися з процесами базового або функціонально орієнтованого функціонування об’єкта.

Найбільш близьким процесом до процесу адаптації є процес розвитку системи. Цей процес в даному випадку будемо розглядати незалежно від можливих типів його прояви. Якщо ввести деяку ієрархію між розглянутими процесами, яка класифікувала їх з точки зору їх можливостей, то на самому верхньому рівні ієрархії варто було б розмістити процеси розвитку, після них можна розмістити процеси самоорганізації і на самому останньому рівні розмістити процеси навчання. У багатьох випадках процеси адаптації і самоорганізації міняються місцями, але це носить виключно методичний характер. Беручи до уваги наведену ієрархію, розглянемо основні фактори, що визначають процеси адаптації. До таких факторів можна віднести наступні:

— мета окремого процесу адаптації носить локальний характер, не визначається заздалегідь і безпосередньо пов’язана з факторами, які ініціюють процес адаптації;

— процеси адаптації, в рамках об’єкта, який змінюється завдяки цим процесам, реалізуються не за рахунок спеціальних коштів, що входять до складу об’єкта, а за рахунок надмірності коштів об’єкта, які можуть брати участь в реалізації основних процесів функціонування об’єкта;

— критерії адаптації, які є складовою частиною мети, в процесі адаптації можуть змінюватися, як в сторону збільшення їх значень, так і в бік зменшення;

— на відміну від процесів розвитку, процеси адаптації не класифікуються за характером змін, які в результаті їх реалізації відбуваються у відповідному об’єкті;

— адаптація, як окремий процес зв’язується з факторами, які його активізують, якщо ці фактори перестали активізувати процес адаптації, то приймається, що адаптація відбулася успішно, якщо відповідні фактори призводять або продовжують приводити до ініціалізації процесів адаптації, то відповідні процеси адаптації не завершилися.

Оскільки кожен процес функціонування об’єкта можна представити у вигляді деяких циклів основних або базових процесів функціонування, то розпізнавання завершеності, незавершеності процесу адаптації пов’язується з періодом основного циклу функціонування. Цей зв’язок полягає в тому, що процес адаптації має відбуватися в межах одного циклу базового процесу функціонування об’єкта. Процеси адаптації, які ініціюються в системі послідовно в часі, можуть призводити до взаємнозворотних станів або можливостям системи. Це означає, що якщо фактор α_i ініціював процес адаптації a_i, а процес a_j, який ініційований фактором α_j, привів систему s в стан, в якому вона була до моменту ініціалізації процесу адаптації a_i, то відповідні фактори називаються контрарними. Якщо два послідовних фактори призводять до процесів адаптації a_i і a_j, які призводять до протилежних, але не рівним за величиною прийнятих критеріїв адаптації, змін в системі, називаються конфліктними або факторами, що визначають чистий конфлікт в системі s. Очевидно, що послідовна в часі реалізація процесів адаптації може призвести до виникнення в системі s процесів розвитку або самоорганізації. При цьому ніяка послідовність процесів адаптації в s не може привести до виникнення процесу навчання в системі Розглянемо деякі системні проблеми, пов’язані з реалізацією процесів адаптації.

Першою такою проблемою є проблема забезпечення виникнення в системі SD процесів адаптації, оскільки відомо, що адаптивність тієї чи іншої системи є внутрішньою властивістю системи SD.

Другою проблемою є проблема розпізнавання фактору виникнення процесу адаптації в s.

Третьою проблемою є проблема аналізу та управління процесами адаптації в рамках системи SD, в якій відповідна адаптація може відбуватися.

Оскільки будь-який з розглянутих процесів не може сам по собі переходити з одного в інший в межах відповідних процесів в рамках наведеної ієрархії їх класифікації, то четвертої проблемою є проблема перетворення системи SD таким чином, щоб сусідні процеси могли переходити один в інший.

Наприклад, якщо процес адаптації позначити $A(s)$, а процеси розвитку і самоорганізації позначити, як $R(s)$ і $C(s)$, відповідно, то можливості переходів одного процесу в інші описується співвідношеннями такого вигляду:

$$[A(s) \to R(s)] \vee [R(s) \to A(s)]$$

$$[A(s) \to C(s)] \vee [C(s) \to A(s)]$$

Доцільність забезпечення можливостей реалізації системою таких переходів обумовлюється тим, що системи, які в даному випадку досліджуються, є системами управління доступом SD, які мають досить тривалими періодами життя, є досить складними і, тому, не можуть часто або, в разі необхідності, замінюватися іншими. В процесі їх експлуатації необхідність в реалізації, в рамках кожної з систем, можливостей форматувати різні процеси, починаючи від процесів навчання до процесів різних типів розвитку може визначатися мінливих умов їх роботи. Природно, що розширення можливостей систем SD зокрема забезпечення реалізації в їх рамках можливостей самоорганізації, адаптації або розвитку, може відбуватися шляхом проведення робіт по відповідній модернізації системи SD, але в цьому випадку виникає задача забезпечення наступності різних версій функціонування системи SD. В даному випадку, мова не йде про створення універсальної системи SD, в якій можуть відбуватися всі наведені процеси, а розглядається можливість реалізації такої SD, для якої можливі часткові переходи з системи одного типу в систему іншого типу. При цьому, розглядаються можливості реалізації переходів в двох напрямках. Часткові переходи систем

одного типу в інший тип не забезпечують повну можливість реалізації в рамках $A(s)$ процесів типу $R(s)$, а виключають можливість виникнення конфліктів в системі, з якої такий перехід реалізується.

Процеси адаптації можуть ввести систему в стан насичення, коли вже не виявляється надлишкових коштів, які можна було б використовувати для подальших процесів адаптації. Крім того, може складатися ситуація, коли зовнішні чинники, які повинні ініціювати процеси адаптації, можуть виявитися не сприйманими системою або чутливість системи до впливів пов'язаних з ініціалізацією процесів адаптації може виявитися недостатньою.

Процес функціонування системи, яка підлягає адаптації, як правило, поєднується з процесами адаптації відповідно до прийнятні дисциплінами розпаралелювання процесів. Тому, важливим завданням для процесів адаптації є контроль їх реалізації з метою виключення можливості виникнення колізій, які можуть привести до порушення роботи системи. У разі, коли такий системою є SD, ініціалізація функціонування якої пов'язана з виникненням запитів на обслуговування, такі колізії можуть призвести до відмови в обслуговуванні або до порушення вимог, що пред'являються з боку користувачів до системи доступу.

Виходячи з викладеного вище, необхідно визначитися з методами адаптації та способами реалізації цих методів, орієнтованих на використання в системах доступу. Оскільки адаптація, як процес внутрішній SD, безпосередньо пов'язаний з параметрами, які мають цілком певну інтерпретацію, процеси адаптації реалізуються в рамках реальних структур доступу, які забезпечують різні рівні захисту і такі процедури пов'язані з відповідними процесами організації доступу.

Система SD, за визначенням, володіє деякими мінімальним рівнем захисту від несанкціонованих користувачів, який, в більшості випадків, ґрунтується на використанні паролів. Таким чином, SD можна розглядати як деяку структуру, яка орієнтована на вирішення внутрішніх завдань захисту і на взаємодію з користувачем, який, в залежності від способу реалізації системи захисту SD, повинен здійснювати діалог що передбачає введення в систему різного типу інформації, яку використовує SD для успішного вирішення завдання захисту

об’єкта доступу від можливості його несанкціонованого використання. Зрозуміло, що, якщо систему захисту *SD* будувати на принципі який складається в збільшенні процесу діалогу *SD* з користувачем, протягом якого користувач буде змушений передавати в *SD* цілком певну інформацію, яку в багатьох випадках досить складно сформулювати, то ефективність такої системи захисту доступу (*SZD*) знизиться до такого рівня, що сама *SD* буде дискредитована. Для вирішення цієї проблеми використовуються такі підходи:

1. проблеми управління рівнем захисту *SD* покладаються на *SZD* і вирішуються згідно з такими методами:

— використовується аналіз історії співпраці окремих користувачів з *SZD*, якщо остання відповідає критерію тривалості співпраці відповідного користувача з системою;

— використовуються уніфіковані протоколи зв’язку між *SZD* і користувачем, які відомі як протоколи доступу [1-6], які досить глибоко досліджені в криптографії;

— використовуються персоніфіковані кошти доступу у вигляді програмно-апаратного обладнання, що є власністю окремого користувача системи доступу;

2. проблеми управління рівнем захисту *SD* вирішуються на основі даних про роботу *SD* протягом заданих моментів часу, які накопичуються в системних засобах управління локальною мережею, яка найчастіше є об’єктом доступу і в цьому випадку використовуються такі підходи:

— зовнішні, по відношенню до системи доступу програмно-апаратні засоби захисту, наприклад системи типу *IDS* [7];

— апаратно-програмні засоби захисту, наприклад Firewall [7, 8], орієнтовані на захист доступу до об’єкта доступу, який здійснюється по каналах зв’язку локальної комп’ютерної мережі з мережею зовнішнього середовища, наприклад мережею Інтернет або іншими локальними мережами;

— використання коштів протидії несанкціонованому вторгненню в систему незалежно від системи *SZD*, які орієнтовані на виявлення потенційних порушень або інтрузії (intrude) і протидії їм;

3. загальні системи управління безпекою локальної мережі, які поряд з іншими засобами забезпечення безпеки мережі, аналізують рівень безпеки ,при цьому, в рамках таких загальних систем вирішуються наступні завдання:

— завдання оцінки рівня безпеки системи доступу до локальної мережі;

— завдання визначення зміни величини ризику завдяки використанню системи *SZD* певного типу або *SZD*, яка характеризується заданими параметрами;

— завдання визначення стійкості *SZD* до можливих атак типу несанкціонованого доступу.

У цьому випадку обмежимося першим підходом, який передбачає вирішувати завдання захисту доступу в рамках коштів системи доступу. Оскільки, в основі реалізації моделей системи доступу буде використовуватися апарат нейронних мереж, то не будемо розділяти систему доступу на частини *SZD* і *SD*. Більш детально зупинимося на відповідних методах.

Метод, який ґрунтується на формуванні історії співпраці з потенційним користувачем, відомий як метод формування профілю користувача. Профіль користувача, по суті, являє собою специфічний спосіб користувача, який складається з параметрів, які характеризують користувача з точки зору його взаємодії з системою. Оскільки, при тривалому використанні обчислювальних ресурсів, потреби в останніх можуть з часом змінюватися, то і відповідний профіль користувача теж може змінюватися. В цьому випадку, одним з найбільш ефективних способів зміни профілю користувача, який, по суті є складовою частиною *SD*, є спосіб, який являє собою процеси адаптації системи доступу до постійно змінюваних параметрів санкціонованого користувача. В цьому випадку, адаптація повинна здійснюватися у вигляді багатопараметричного процесу, оскільки відредагування параметрів профіля користувача можуть відбуватися в зв’язку зі спробами фальсифікації легального користувача. Цю можливість

повинна відстежувати процедура, яка реалізує відповідну адаптацію SZD. Реалізація відповідного методу адаптації вимагає використання цілого ряду параметрів, до яких можна віднести:

— час актуалізації профілю користувача;

— швидкість зміни параметрів користувача;

— синхронізація процесів зміни параметрів із зовнішніми або внутрішніми параметрами SD;

— межі значень змінних параметрів;

— ступінь знайомства користувача з об’єктом доступу;

— зміна індивідуальних особливостей користувача і цілий ряд інших ознак користувача, які можуть використовуватися в якості параметрів, аналізованих системою SD

Наведені параметри, які аналізуються, при реалізації процесів адаптації, не є параметрами самого процесу адаптації, а характеризують компоненти або дані SD, які піддаються змінам. Оскільки зміни в можуть відбуватися і незалежно від процесу адаптації, наприклад, при введенні в SD будь-якої інформації системними службами мережі і системи безпеки в цілому, то необхідно більш чітко визначити процес адаптації як такої. Це є необхідним ще й тому, що, як зазначалося вище, процеси адаптації можуть переходити в процеси розвитку або процеси самоорганізації, які необхідно розділяти, оскільки вони мають свої особливості. Тому, визначимо процес адаптації, щоб в рамках даної роботи дослідити його, не переходячи з цього процесу в інші типи процесів, що може привести до невизначеності отриманих результатів відповідних досліджень.

Визначення 5.1. Процесом адаптації в системі SD є процес, який регламентується наступними співвідношеннями:

— процес адаптації може виробляти зміни оцінки значень аналізованих параметрів;

— процес адаптації не здійснює зміни логіки алгоритмів аналізу контрольованих параметрів;

— процес адаптації може змінювати кількість аналізованих параметрів, якщо це не призводить до змін логіки аналізу окремих параметрів.

Виходячи з наведеного визначення видно, що в процесі адаптації не здійснюється структурних змін системи аналізу об'єктів.

Наведені вище можливі дії процесів адаптації можуть ініціалізуватися тільки при виникненні або виконанні певних умов. В іншому випадку будуть порушені принципи реалізації процедур контролю і, відповідно, порушиться захист безпеки об'єкта доступу. Розглянемо ряд умов, які повинні виконуватися для того, щоб могли реалізовуватися дії в SD, класифікуються як дії процесів адаптації.

Розглянемо умову, що визначає допустимість зміни оцінки значення аналізованого параметра p_i.

Умова 5.1. Оцінка параметра p_i в SD може бути змінена на величину Δ_i, якщо має місце співвідношення:

$$\forall n(p_i)[\alpha_i \geq p_i \geq \beta_i] \& [\alpha_i \geq \alpha + \delta(\alpha)] \& [\beta_i \leq \beta - \delta(\beta)] \rightarrow (\alpha = \alpha_i) \& (\beta = \beta_i)$$

де α і β граничні значення діапазону значень параметра p_i, α_i - перевищення межового значення α або нова верхня межа, β_i - нова нижня межа β значення параметра p_i, n - кількість випадків перевищення значень параметра p_i верхнього допустимого значення.

Наведена умова ініціалізації процесу адаптації відповідає випадку модифікації межових значень контрольованих параметрів і відноситься до випадку реалізації в SD порогових алгоритмів контролю доступу. Очевидно, що крім порогових алгоритмів контролю значень параметрів можуть використовуватися і інші, більш складні алгоритми контролю, наприклад, алгоритми контролю швидкості зміни значень параметрів протягом певної кількості звернень користувача до SD і т.п. Чимало атак на комп'ютерні системи містять механізми повторення одних і тих же, дій, що направлено на фальсифікацію умов типу умови 5.1. Відповідно до нього, якщо вводиться параметр p_i n раз в SD, значення якого лежить в межах $[\alpha_i, \beta_i]$, тоді на $n+1$ раз

відповідне значення будуть сприйматися як допустимі. Вирішення цієї проблеми здійснюється наступними способами:

— використовується зворотний зв'язок між SD і об'єктом доступу (OD), по якій передаються дані про допустимість p_i з точки зору засобів захисту окремих компонент OD;

— на параметри системи SD проектуються зміни, які відбуваються в OD і не пов'язані з завданнями захисту, що може призводити до зміни оцінок значень параметрів доступу p_i;

— вирішується завдання прогнозування змін в SD, які проектуються на відповідні параметри захисту p_i, що може призвести до переоцінки їх поточних значень.

Звісно, що можуть існувати й інші механізми аналізу допустимості зміни значень параметрів захисту в SD, наприклад, механізми, які ґрунтуються на імітації реакції OD на змінені параметри захисту і т.д.

5.2. Дослідження способів реалізації процесів адаптації в нейронних мережах

Важливою особливістю процесів адаптації системи доступу (SD) є зміна кількості параметрів, які реалізуються в системі. Очевидно, що ініціація реалізації такої можливості повинна відбуватися відповідно до визначеного умовою. Сформулюємо таку умову таким чином.

Умова 5.2. Кількість m параметрів P_i в SD може бути збільшено на величину K, якщо має місце наступне співвідношення:

$$\forall k \exists B(x_1, x_2, \cdots, x_N)\left[\left[\left(B \to P_{jk}\right) \& \left(s \to \left[s^* = f_k\left(s, P_{jk}\right)\right]\right)\right]\right] \to \left(P_{jk} \in SD\right),$$

де $B(x_1, x_2, \cdots, x_N)$ - система формул описує процеси визначення несанкціонованого доступу до SD, s^* - система захисту, в якій передбачається виконання аналізу P_{jk} відповідно до функції f_k. Виходячи з цієї умови можна припустити, що система

$B(x_1, x_2, \cdots, x_N)$ містить всі параметри P_{jk} , які можуть бути включені в систему Насправді система B являє собою логічні формули, які формуються незалежно від SD на основі аналізу інтерпретаційних розширень зовнішнього середовища, в якому функціонує мережа. Будь-яка локальна мережа не формується виходячи з абстрактних вимог, а формується таким чином, щоб вона відповідала особливостям її використання потенційними споживачами або завданнями, які на ній передбачається вирішувати.. Традиційно ці дані знаходять свого безпосереднього відображення в рамках мережі, а залишаються, в кращому випадку, в проектній документації на мережу. В рамках даного підходу, ця інформація повинна міститися в засобах мережі в силу наступних причин:

— для реалізації прогресивних методів вирішення завдань захисту інформації в мережі і захисту самої мережі,

— для вирішення завдань автоматизованої модифікації мережі в разі змін у зовнішньому середовищі, на яку орієнтована мережа,

— для забезпечення адекватності мережі і її можливостей до зовнішнього середовища, яку мережу обслуговує і т.д.

Таким чином, якщо з'являється необхідність збільшити рівень безпеки мережі, то користувачеві, якщо він входить до складу зовнішнього середовища на яку орієнтована мережа, пропонується з боку SD, під час чергового сеансу зв'язку, використовувати додатковий параметр P_j для того, щоб він міг отримати доступ до OD, який організовується системою доступу. Звісно, що таким параметром може не володіти користувач, який до цього моменту ідентифікувався системою доступу, як санкціонований користувач, але тоді питання про збереження попереднього статусу користувача або процесу переноситься в сферу завдання визначення, якою мірою даний користувач може бути віднесеним до зовнішнього середовища, на яку орієнтована захищувана мережа. Може виникнути питання про те, яке відношення має SD до інших систем, які можуть бути присутніми в мережі або не бути присутнім в ній. Справа полягає в тому, що SD не може вирішувати оригінальні завдання захисту доступу в рамках системи

що представляє собою якщо остання за своїм рівнем розвитку, не відповідає рівню можливостей, які закладаються всі компоненти в даному випадку, в систему доступу.

Умова 5.3. Кількість m параметрів P_i в SD може бути зменшено на K, якщо виконується наступне співвідношення:

$$\forall K \exists \left[u\left(s^*\right) \geq u(c) \right] \exists s\left(P_1,\cdots,P_N\right) \left[\left[s\left(P_1,\cdots,P_N\right) \to s^*\left(P_1,\cdots,P_{N-K}\right) \right] \& \, SD\left(s^*\right) \right] \to SD \setminus \sum_{N-K}^{N} P_j.$$

де $u\left(s^*\right)$ - опис рівня безпеки, який забезпечує система SD;

$u(c)$ - опис рівня безпеки SD, який визначений як мета;

$s\left(P_1,\cdots,P_N\right)$ - система захисту, яка входить в SD і здійснює захист OD із заданим рівнем $u(c)$;

$s^*\left(P_1,\cdots,P_{N-K}\right)$- логічна система аналізу безпеки доступу, яка може бути виведена з $s\left(P_1,\cdots,P_N\right)$.

У цьому співвідношенні, як і в попередньому, теж використовується зовнішня функція $u(c)$, яка не належить до системи SD, а характеризує систему OD в цілому. Неминучість розширень такого типу в уявленнях про рівні безпеки, який забезпечується системою SD, обумовлюється тим, що SD є складовою частиною мережі або OD і говорить про те, що SD забезпечує рівень безпеки, який не пов'язаний з рівнем безпеки OD, некоректно.

Умовами ініціації модифікації SD можуть виступати наступні фактори:

— відсутність спроб несанкціонованого доступу, які могли бути виявлені системою SD протягом реалізації m запитів на доступ до OD через SD,

— зміна рівня безпеки мережі або OD в силу змін у зовнішньому середовищі що описується системою логічних функцій $B\left(P_1,\cdots,P_N\right)$,

— невідповідністю між рівнем захисту, який забезпечує SD і параметрами, які контролюються системою, при виникненні запитів на доступ до OD з боку користувача або процесу.

Перший фактор характерний для систем, які мають властивості адаптації, властивостями самоорганізації або іншими властивостями, що визначають

високий рівень організації SD і OD в цілому. Доцільність використання цього фактору визначається тим, що процедури контролю доступу в залежності від своєї складності вимагають більше або менше обчислювальних ресурсів, їх реалізація та адекватне виконання вимагає тим більше часу, чим більша кількість параметрів користувача необхідно перевіряти. Одна з найважливіших причин, які обумовлюють доцільність зменшення P_i, за якими ідентифікується користувач і визначається його повноваженнями в OD, є спрощення доступу до системи з боку користувача.

Звичайно вимагати зменшення рівня захисту, яка забезпечується SD, якщо загальні вимоги до рівня захисту OD були зменшені. В даному випадку, не зупинятимемося на аналізі причин, за якими такі вимоги зменшуються, але це не означає, що відповідна ситуація по відношенню до мережі не можлива або не виникає.

Параметри, які контролюються системою SD, не є абстрактними, а мають певну інтерпретацію в області завдань захисту, які вирішуються в SD. В рамках такої інтерпретації визначається значимість параметра в рішенні задач ідентифікації, допустимі значення його величини, ймовірність його оригінального походження і т.д. Очевидно, що логіка роботи SD тісно пов'язана з відповідними інтерпретаціями P_i і дозволяє визначити внесок того чи іншого параметрів в забезпечення заданого рівня захисту. Завдяки таким даними в рамках SD, існує можливість формування критеріїв для визначення тих параметрів, які можна було б виключити з аналізу, щоб привести реалізований в SD рівень захисту у відповідність зі зміненими до захисту вимогами.

Можна виділити досить багато аспектів, які пов'язані з реалізацією систем адаптації. Кількість таких аспектів тісно пов'язане з кількістю розглянутих предметних областей. Проте, необхідно проаналізувати ще й такі аспекти, які є загальними для системи що володіють властивостями адаптації:

— визначити цілі процесів адаптації;

— визначити тривалість процесів адаптації;

— визначити можливості методів адаптації в рішенні задач забезпечення безпеки *SD*, при змінних факторах, які ініціюють або пов'язані з процесами адаптації.

Цілі процесів адаптації можна розділити на:

— локальні цілі;

— інтегральна мета;

— умовні або виділені цілі.

Локальні цілі передбачають проведення такої адаптації *SD*, після якої остання могла б виявляти і протидіяти черговим несанкціонованим кількість звернень на отримання доступу. При цьому, такі методи несанкціонованого доступу повинні ставитися до класів, які ще не розпізнавала система *SD*. Така мета може бути представлена, як мета що полягає у формуванні нового образу атаки на *SD*. Досить аргументованим може бути твердження про те, що нова можлива атака на *SD* є розвитком або певним ускладненням відомих атак. В цьому випадку, можна говорити про виведення опису нової атаки на основі даних про вже відомих атак. Для цього, необхідно розглянути можливі розширення допустимих перетворень в нейронній мережі, які дозволили б реалізовувати відповідні висновки описів атак.

Інтегральна мета полягає в таких змінах в *SD*, які будуть забезпечувати ефективнішу здатність *SD* до виявлення нових атак. Прикладом підвищення такої ефективності може служити використання і реалізація алгоритмів прогнозу зміни значень параметрів, які можуть характеризувати нові атаки на *SD*. В даному випадку, найбільш доцільно моделі прогнозування будувати на основі кривих розвитку або інших однопараметричних функціях, які дозволяють передбачати такі зміни параметрів атак, які визначають нові атаки. Другим прикладом інтегральної мети процесів адаптації *SD* може служити збільшення ефективності протидії атакам. Здатність засобів захисту до протидії атакам є їх істотною особливістю особливо, якщо врахувати, що найпростіший спосіб протидії являє собою переривання процесу доступу. Наступним прикладом інтегральної мети коштів адаптації може служити збільшення швидкості розпізнавання атаки і т.д.

Рішення завдання збільшення швидкості розпізнавання атаки може ґрунтуватися на наступних підходах:

— на формуванні ієрархії параметрів окремої атаки, а також ієрархії між атаками;

— на підставі аналізу історії атак на SD і т.д.

— визначення інших інтегральних ознак може ґрунтуватися на уточненні предметної області інтерпретації процесів функціонування SD.

Можливість існування умовних або виділених цілей обумовлюється додатковими вимогами, які можуть формулюватися по відношенню до об'єкта захисту або самої SD. Прикладом таких умов або вимог можуть служити:

— умови зі зміни параметрів реалізації доступу, якими можуть виступати також і паролі;

— умови по зміні процедур доступу для виділених груп користувачів або процесів;

— умови, що визначають необхідність зміни рівня захисту доступу і т.д.

Очевидно, що функціонування SD, відповідно до виконання додаткових умов, може здійснюватися і в рамках загальної організації процесів адаптації. Різниця між цими двома випадками полягає в тому, що, в першому випадку, додаткові цілі сформовані зовнішніми факторами, до яких, в першу чергу, відносяться адміністратори безпеки.

Функціонування системи, яка орієнтована на виконання певних завдань, в даному випадку, завдань організації доступу до обчислювальних засобів, не може безперервно супроводжуватися процесами адаптації. Процеси адаптації, які призводять до певних змін в SD, повинні реалізовуватися тільки в певні періоди часу функціонування. При цьому, можливі наступні режими реалізації процесів адаптації:

— автономний спосіб реалізації процесу адаптації системи SD;

— поєднаний спосіб реалізації процесів адаптації.

У першому випадку процеси адаптації в часі розділені з процесами управління доступом. Цей режим, найчастіше використовується при реалізації

локальних цілей адаптації, особливо, якщо останні формуються зовнішніми факторами.

Поєднаний спосіб реалізації процесів адаптації полягає в поділі процесів адаптації і процесів функціонування та їх виконання в одному з можливих режимів функціонування обчислювальних засобів, наприклад, в мультипроцесорному режимі. Цей спосіб реалізації процесів адаптації використовується в тому випадку, якщо обслуговування користувачів не повинно перериватися, при виникненні локальних цілей адаптації або виділених цілей.

Фоновий спосіб реалізації процесів адаптації використовується в тому випадку, коли визначена інтегральна мета, на досягнення якої може знадобитися більше часу, по відношенню до часу, який необхідний для досягнення локальних або виділених цілей. Необхідність в цьому обумовлюється тим, що інтегральна мета описується в вигляді складових її локальних і умовних цілей, послідовність досягнення яких визначається структурою інтегральної мети. Прикладом інтегральної мети може служити мета яка полягає в збільшенні рівня захищеності від атак певного типу і т.д. скільки система доступу і система захисту доступом реалізуються на основі використання структур нейронних мереж, а окремі фрагменти нейронних мереж мають відокремленою, в певному сенсі, функціональної орієнтацією, то фоновий спосіб реалізації процесу адаптації полягає в тому, що процеси адаптації ініціалізуються в одних фрагментах нейронної мережі, а процеси обслуговування доступу і процеси контролю, які пов’язані з забезпеченням захисту реалізуються в інших фрагментах нейронної мережі. Така можливість фрагментації пов’язана з можливістю досить найрізноманітнішої інтерпретації небезпек, які існують по відношенню до SD, типів атак, які можуть реалізовуватися, різних груп користувачів звертаються до SD, різними типами послуг, які можуть надаватися об’єктам захисту тощо.

Беручи до уваги викладене вище, необхідно визначати час протікання процесів адаптації. Оскільки, кожен окремий процес адаптації пов’язаний з метою

відповідних змін *SD*, то необхідно аналізувати міру досяжності відповідних цілей. Одним із способів визначення міри досяжності процесом адаптації деякої мети є визначення часу, протягом якого цей процес адаптації здійснюється. Оскільки процес адаптації відбувається не тільки у відповідності з лінійними алгоритмами, які передбачають тривіальні перетворення, а в залежності від рівня функціональних можливостей механізмів адаптації, може являти собою алгоритм відповідний нелінійним перетворенням або алгоритмам із зворотними зв'язками, то ініційований процес адаптації може призводити до наступних ситуацій:

— нормальному завершенню процесу адаптації, яке відповідає досягненню локальної мети;

— зациклення процесу адаптації, якщо алгоритм відповідно до якого реалізується адаптація, містить зворотні зв'язки;

— переходу в тупикову ситуацію, коли процес адаптації завершився, але при цьому локальна мета виявилася досягнутою;

— завершення процесу адаптації, при якому в результаті перетворень вихідні параметри, на підставі яких формувалася локальна мета, погіршилася.

Нормальне завершення процесу адаптації визначається в описі мети, яке описує відмінність стану, до якого повинна привести адаптація від стану, в якому знаходиться до моменту ініціації процесу адаптації відповідний фрагмент системи *SD* і, відповідно, фрагмент нейронної мережі. Таким чином, в рамках даного підходу, адаптація всієї нейронної мережі реалізується у вигляді здійснення процесів адаптації в різних фрагментах мережі, і представляє собою певне узагальнення всіх окремих процесів адаптації, що відбуваються за певний інтервал часу в мережі в цілому. У зв'язку з цим, можна говорити про розподіл процесів адаптації в нейронній мережі і, відповідно, в системі *SD*. У найпростішому випадку під узагальненим процесом адаптації можна розуміти суму всіх процесів адаптації що відбуваються в мережі віднесена до всіх фрагментів нейронної мережі за певний інтервал часу функціонування мережі, що формально можна записати у вигляді співвідношення:

$$A(S) = \left[\left[\sum_{i=1}^{m} A_i(S_i) \right] / n \right] \cdot \Delta T_i,$$

де m - кількість фрагментів S_i нейронної мережі S, в яких протягом інтервалу ΔT_i відбулися процеси адаптації $A_i(S)$, n - загальна кількість фрагментів в мережі S.

Зациклення процесу адаптації є найбільш небезпечним наслідком ініціації процесу адаптації оскільки в цьому випадку ініційований в деякому фрагменті процес ніколи не завершитися. Це може привести до блокування можливості ініціації основних процесів управління доступом в рамках відповідного фрагмента SD. Тому, одним з основних засобів запобігання таких наслідків рішення локального завдання адаптації, є контроль часу реалізації процесу адаптації. В цьому випадку, тривалість процесу адаптації є важливим параметром, що підлягають контролю. У зв'язку з цим, в рамках моделі адаптації повинна вирішуватися завдання визначення часу протікання відповідного процесу. З цим параметром досить тісно пов'язаний параметр, який характеризує момент ініціації процесу адаптації. Справа в тому, що на відміну від класичних уявлень про процеси адаптації, в нейронних мережах в рамках нейронних моделей використовуваних для вирішення завдань захисту SD, процеси адаптації носять локальний характер, як в рамках нейронної мережі так і в часі. Отже, умови ініціації цих процесів і моменти їх виникнення, в рамках всієї системи SD повинні містити описи, в яких визначені фрагменти, в яких необхідно ініціювати процеси адаптації. Отже, будь-який локальний процес адаптації пов'язаний з інтегральними умовами ініціації цих процесів в нейронної мережі, що відповідає загальноприйнятій ідеології перетворень в таких мережах.

Безвихідна ситуація є специфічною для випадку використання нейронних мереж, оскільки вона полягає в тому, що процес адаптації ініційований і завершений, але поставлені перед ним цілі не досягнуті. Можна було б вважати, що існування безвихідної ситуації є суперечливим для випадку реалізації і аналізу процесів адаптації в нейронних мережах, оскільки процеси адаптації

розглядаються як зміни, які призводять до поліпшення показників функціонування мережі по відношенню до тих чи інших критеріїв. В даному випадку, доцільність виділення безвихідних результатів перетворень, які здійснюються процесами адаптації, ґрунтується на тому, що ці процеси розглядаються як локальні і тим або іншим чином реалізують свій внесок в процеси адаптації, які в нейронної мережі відбуваються в цілому. Це означає, що якщо за інтервал часу ΔT_i в системі S мала місце $A(S)$, то окремі $a_i(s_i) \in A(S)$, які завершилися безвихідними ситуаціями, в цілому не дискредитують $A(S)$. Отже протягом довільного періоду ΔT_i протягом усього часу функціонування S повинно мати місце співвідношення:

$$\forall \Delta_i T\,[A(S) = \sum_{i=1}^{K} a_i(s_i) + \sum_{j=1}^{m} a_i(s_i)] \rightarrow [\sum_{i=1}^{K} a_i(s_i) < \sum_{j=1}^{m} a_i(s_i)].$$

Якщо безвихідна ситуація виникає в одному фрагменті нейронної мережі і це не призводить до зміни співвідношення $\sum_{i=1}^{K} a_i(s_i) = \sum_{i=1}^{m} a_i(s_i) + \alpha$, де α - деякий коефіцієнт пропорційності, який може змінюватися в заданих межах, наприклад, $[\alpha_1, \alpha_2]$, то окремий процес $a_i(s_i)$ тільки реєструється. Якщо наведена рівність порушується таким чином, що:

$$\sum_{i=1}^{K} a_i(s_i) > \sum_{j=1}^{m} a_i(s_i) + \alpha,$$

то система управління процесами адаптації повинна не тільки фіксувати факти виникнення безвихідних завершень, а й відновлювати узагальнений процес адаптації.

Виходячи з викладених уявлень про безвихідні завершення процесу адаптації, можна стверджувати, що в рамках нейронної мережі повинні формуватися спеціалізовані вузли, що реалізують функції:

— ініціації процесів адаптації;

— контролю часу функціонування;

— аналізу умов завершення локального процесу адаптації;

— зв’язку фрагментів локальних процесів адаптації з інтегральними умовами узагальненого процесу адаптації в рамках всієї системи SD.

Завершення процесу адаптації, при якому параметри, що описують мету, змінилися в бік погіршення, що визначається умовами мети, являє собою випадок посилення наслідків впливу процесу адаптації на нейронну мережу в порівнянні з його безвихідним завершенням. Такий випадок завершення процесу адаптації, на відміну від завершення безвихідною ситуацією, вимагає додаткових впливів з боку системи на процеси адаптації в період їх реалізації, а також вимагає додаткового аналізу умов ініціації процесів адаптації та умов їх виконання. Це означає, що в рамках системи, яка дає змогу адаптації повинна існувати деяка підсистема або, щонайменше, спеціальні засоби псевдоуправління процесу адаптації. Під псевдоуправлінням, в даному випадку, мається на увазі аналіз всіх вихідних даних, які визначають процес адаптації і їх модифікацію, яка може здійснюватися в такий спосіб:

— безпосередньо перед виконанням чергового локального процесу адаптації;

— по завершенню процесу адаптації, який завершився погіршенням значень параметрів, що визначають мету процесу адаптації.

5.3. Аналіз основних параметрів процесу адаптації та їх формальний опис

Однією з особливостей нейронних мереж є їх однорідність і розподіленість. Коли мова йде про розподіл, то перш за все мають на увазі її просторовий розподіл. Властивість однорідності не допускає існування функціонального розподілу. Це означає, що всі необхідні функціональні можливості всієї мережі повинні бути локалізовані в кожному фрагменті мережі, який є елементарним для нейронної мережі. Другою особливістю мережевих структур є те, що вони не передбачають існування елементів, які були б спільними для всієї мережі. З цього випливає, що загальна оцінка стану мережі здійснюється поза самої мережі, на основі даних про параметри, що характеризують всю мережу.

Розглянемо методи модифікації базових елементів нейронних мереж, з метою забезпечення можливості реалізації процесів адаптації в рамках окремих елементів мережі. У цьому сенсі, адаптацію можна розглядати, як адаптацію локальну. В даному випадку, уявлення про адаптації має на увазі такий процес, який може бути оцінений, як позитивний з точки зору інтегральних критеріїв, які є характерними для процесів і завдань, що вирішуються в досліджуваних системах. В даному випадку, мова йде про збільшення безпеки системи доступу. Принципи реалізації локальної адаптації повинні відповідати таким вимогам до адаптаційних процесів, які можуть відбуватися в мережі:

— локальна адаптація не повинна призводити до виникнення протиріч між окремими елементами нейронної мережі;

— адаптація не повинна призводити до виникнення конфліктів між процесами, які реалізують процедури управління доступом, що реалізуються в різних фрагментах мережі;

— локальна адаптація повинна реалізовуватися таким чином, щоб сукупність процесів такої адаптації, по принаймні, в межах певного інтервалу, який в порівнянні з інтервалами часу, протягом яких реалізуються окремі процеси адаптації, були б значно більшими, і щоб в рамках своєї системи, перебіг передвиборних процесів локальної адаптації, в рамках цієї системи приводили б до підсумкових змін, які могли б бути інтерпретовані, як зміни адаптаційного характеру;

— адаптація, з точки зору критеріїв, на локальному рівні повинна допускати інтерпретацію позитивних змін в рамках цілей, для яких використовуються дані процеси і методи.

У зв’язку з викладеною специфікою реалізації процесів адаптації, необхідно розглянути критерії та умови, яким повинні відповідати процеси адаптації, що володіють зазначеними особливостями. До підходів, які в найбільшій мірі можуть відповідати наведеним вище особливостей можна віднести наступні:

— підходи використовують уявлення про функції корисності [9, 10];

— підходи, в основі яких лежать уявлення про теорію перспектив;

— підходи, які ґрунтуються на використанні уявлень про ризик;

— підходи, які ґрунтуються на використанні механізмів штрафів і нагород;

— підходи, які ґрунтуються на використанні коштів, що дозволяють визначати кількість інформації, що з'являється в результаті реалізації процесів адаптації.

Поняття про функції корисності розглядалися в зв'язку з дослідженнями в теорії ігор [9, 11-14]. Однією з важливих задач теорії ігор є завдання вибору чергового ходу одним з гравців, який повинен забезпечити йому виграш. У найпростішому випадку, приймається, що ймовірність вибору ходу, в результаті якого можна отримати результат гри $x_1, ..., x_n$ дорівнює, відповідно $p_1, ..., p_n$. В цьому випадку можна записати:

$$EU = \sum_{i=1}^{n} P_i \, U(x_i), \tag{5.1}$$

де $U(x_i)$, функція, яка додатково оцінює очікувану вартість гри.

Ця функція для кожного окремого учасника гри може бути різною. В рамках нейронної системи, така функція може бути індивідуальною для окремого локального фрагмента мережі. Використання індивідуальних функцій дозволяє розглядати ряд випадків, як сходиться ряд. Наприклад, якщо взяти в якості опції $U(x)$ функцію $\log_{10} 2^n$, то вартість очікуваної корисності

$$EU = \sum_{i=1}^{n} (1/2)^n \log_{10} 2^n,$$

сходиться до очікуваної кордоні вартості гри. При дослідженні теорії корисності в рамках теорії ігор, Фон Нейман і Маргенштерн довели твердження, в якому йдеться про те, що можна сформувати аксіоми для прийняття рішень, які забезпечують досягнення максимальної очікуваної корисності. Це твердження означає, що при виконанні певних умов існують функції корисності, які можна використовувати в рамках співвідношення (5.1). Оскільки функції корисності розглядалися в зв'язку з дослідженням систем, в яких бере участь користувач, то досліджувалася функція суб'єктивної корисності, яка описується співвідношенням:

$$SEU = \sum_{i=1}^{N} S_i U(x_i),$$

де S_i - суб'єктивна ймовірність, за умови, що $\sum_{i=1}^{N} S_i = 1$. У разі систем доступу, які орієнтовані на обслуговування користувачів, така суб'єктивна ймовірність відображає особливості окремого користувача, які реєструються в SD. Використання цього підходу вимагає реалізації механізмів накопичення значень параметрів, які визначають профіль користувача. При цьому, функція корисності може в процесі адаптації модифікуватися, що відображає сам процес адаптації локального елемента мережі.

Вибір критеріїв адаптації може ґрунтуватися на поняттях теорії перспектив. У цій теорії, як і теорії корисності, мова йде про способи прийняття рішень, що є більш ефективним в порівнянні з використанням простих критеріїв. В рамках теорії перспектив, процес прийняття рішення, фактично складається з двох компонент - компоненти набуття досвіду і компоненти безпосереднього прийняття рішення. Відповідно до подання про теорію перспектив приймається, що оцінюється кожен вибір і здійснюється вибір того варіанта, який має найбільшу вагу. Така вага визначається двома ваговими функціями $\pi(p)$ і $v(x)$, де $\pi(p)$ пов'язане з ймовірністю p, а друга $v(x)$ відображає суб'єктивну вартість вибору x. Формально, така функція вибору описується співвідношенням:

$$V(x, p, y, q) = \pi(p)\, v(x) + \pi(y)\, v(y).$$

В рамках цього підходу, заміна ймовірності p ваговою функцією $\pi(p)$ являє собою узагальнення традиційної концепції корисності.

В теорії корисності і теорії перспектив вирішується завдання, яке описує, як реалізується процес прийняття рішення. При цьому, не менш важливим є нормативні проблеми, які полягають у тому, щоб визначити чисельні методи визначення вагових функцій $\pi(p)$ і $v(x)$.

Для дослідження функції нормативного підходу до прийняття рішень, необхідно більш детально розглянути концепцію двохфакторну функцій корисності. В рамках цього підходу необхідно визначитися з функцією мети, на

основі якої можна було б оптимізувати довго періодичну стратегію управління процесами адаптації. Така функція, яка називається функцією корисності збалансованого розвитку $U(x)$, повинна враховувати зовнішні мотивації елемента приймає рішення, які пов'язані з розглянутими рішеннями про розвиток і виражаються за допомогою величини параметрів зворотного зв'язку Ru, а також ймовірності досягнення успіху p і значень параметрів, що визначають можливість виконання процедур адаптації, які визначаються співвідношенням $X = I / P,$ де P - величина значень параметрів, які на момент початку процесу вже визначені значеннями факторів, які на момент ініціації процедури адаптації вже використовувалися раніше. У загальному вигляді така функція запишеться у вигляді співвідношення:

$$U(x) = F[Z, Y],$$

де $Z = PRx$ - очікуваний успіх, в результаті реалізації процесу адаптації, який може бути досягнутий завдяки $I = Px,$ а $R = pRu$ - величина зворотного зв'язку, яка забезпечить можливість використовувати результати процесу адаптації на чергових етапах використання відповідного фрагмента мережі. Ця величина ґрунтується на моделі розподілу випадкової змінної $\overline{R}$:

$$R = [(P_m - I) / I] = [(E : P) \to (Ru > 0)] \vee [(E : (1 - p)) \to R_{0l} = 0],$$

де P_m - змінна, імовірнісна величина значення параметра, що визначає збільшення успішного використання фрагмента мережі, при вирішенні задач управління доступом.

Фактор $Y = PR - Pk\sigma$ - становить гарантовану величину успіху, σ - дисперсія, яку визначають в рамках даного підходу як величину ризику. Параметр k визначає вагу стандартного відхилення σ і залежить від нижньої межі ймовірності успішних результатів $\overline{P}$, або:

$$k \le 1(\sqrt{1 - \overline{P}}).$$

Оскільки функція F повинна забезпечувати нормалізацію або приведення факторів Z і Y, то вона повинна бути гомогеніческа. Тому, приймаємо, що

$$U(x) = Z^{\beta} Y^{1-\beta} = PRS^{(1-\beta)} x^{\beta},$$

де $S = 1 - K\sigma / R,\ \ \beta \in (0,1),$ що гарантує, що $U(x)$ є функцією увігнутою. Увігнутість функції $U(X)$ гарантує оптимізацію існуючих можливостей P, які на даний момент вже використовуються в n випадках функціонування відповідного фрагмента, що характеризує корисність, яка описується в такий спосіб:

$$U_i(x_i) = PR_i S_i^{1-\beta} x_i^{\beta};\ \ S_i = 1 - k_i\sqrt{(1/P_i) - 1}.$$

Це забезпечує вирішення проблеми:

$$\max_{X_i \in \Omega} \sum_{i=1}^{n} U_i(x_i);\ \ \Omega = \left\{ x_i \Big/ \sum_{i=1}^{n} x_i = 1,\ \ x_i \geq 0 \right\}.$$

Щоб можна було обчислити величину $U(x_i)$, необхідно ідентифікувати параметр β, який являє собою вагу, яка пов'язує процес прийняття рішення з фактором Z. Така ідентифікація може ґрунтуватися на наступних двох положеннях.

Перше положення являє собою еквівалент впевненості. Це означає, що

$$U(x) = PRS^{1-\beta} x^{\beta},$$

де R величина вартості поліпшення роботи за умови, що прийняте рішення, при зміні ваги одного з входів нейрона, не принесе очікуваної корисності $U(x)$. Ця величина $U(x_i)$ повинна бути що дорівнює величині корисності $U_F(x_F)$, збільшення якої не підлягає ризику

$$U_F(x_F) = PR_F x_F^{\beta}.$$

З умови рівності цих показників корисності можна записати співвідношення:

$$x_F / x = S^{(1-\beta)/\beta} (R / R_F)^{1/\beta}.$$

Друге положення полягає в поділі збільшення позитивних змін на витрати пов'язані з компенсацією величини можливого ризику, які записуються у вигляді $I = h\Delta P,$ де h - одиниця зміни величини компенсації, і витрати пов'язані з резервуванням зміни вхідних ваг, які забезпечують корисність

$$U_F(1-h) = \Delta P R_F (1-h)^{\beta}.$$

Виходячи з умов досягнення максимальної корисності, можна оптимальну стратегію отримати з наступних умов:

$$\beta \Delta PRS^{1-\beta} h^{\beta-1} - \beta \Delta PR_F (\beta - 1)\, h^{\beta-1} = 0.$$

Після перетворення цього співвідношення отримаємо

$$\beta = [1 + [(\ln (X_F / X) / (\ln (h/(1-h)))]].$$

В основі інформаційного підходу прийняття рішення по модифікації нейрона з метою його адаптації лежить концепція ентропії, як міри невизначеності механізму прийняття рішень, яка виражає міру хаосу в безлічі варіантів розвитку фрагмента мережі, який виражаються можливостями успіхів або втрат, пов'язаних з цими виборами варіантів розвитку. Нехай дані про можливі варіанти вибору представляються у вигляді множини $X = \{x_1, ..., x_n\}$, тоді множина:

$$P_\gamma(x) = \{P(x_1, ..., P(x_n)\}$$

визначає ймовірність, що той варіант став відомий системі прийняття рішень, що відповідає принципу Шенона [15], який визначає поняття ентропії. Величину відповідної інформації прийнято позначати як $I(X_i)$, тоді, відповідний принцип можна описати у вигляді наступного співвідношення:

$$P(x_i) > P(x_K) \Rightarrow I(x_i) < I(x_K), \qquad (5.2)$$

де стрілка «$\Rightarrow$» означає «тоді і тільки тоді». Розглянемо ситуацію, коли є дві множини інформаційних повідомлень X і $Y = \{y_1, ..., y_m\}$, при цьому, величину інформації для першого джерела позначимо $f[P(x_i)]$, де f це функція $P(x_i)$. Величина інформації для другого джерела визначається у вигляді $f[P(x_j / x_i)]$, де $P(Y_j \mid x_i)$ являє собою умовну ймовірність.

Друге поняття, яке вводиться в [15] полягає в тому, що в разі існування двох залежних ймовірностей, появи відповідних відомостей x_i і y_i, які на даний момент обрані; функція f повинна задовольняти співвідношенню:

$$f[p(y_j \mid x_i)\, p(x_i)] = f[p(y_j \mid x_i)] + f[p(x_i)].$$

Якщо позначити $p(y_j \mid x_i)$ символом «a», а $p(x_i)$ - символом «b», то відповідна умова записується у вигляді

$$f[a, b] = f(a) + f(b).$$

Ця умова забезпечується логарифмічною функцією $f(a) = k \log a$, де k - константа. Тому, можна записати, що $I(x_i) = f[p(x_i)] - k \log p(x_i)$. Беручи до уваги (5.2), можна записати $I(x_i) = -\log p(x_i)$. В цьому випадку, міра невизначеності для всієї множини даних X може бути записана у вигляді:

$$UC(X) = -\sum_{i=1}^{n} p(x_i) \log p(x_i).$$

Виходячи з уявлень щодо умовної ймовірності, можна оцінити вплив другого джерела даних на дані з першого джерела, яке, спричинить за собою зміну невизначеності впливає на прийняття рішення, метою якого є досягнення максимальної корисності процесів адаптації. В цьому випадку, відповідну функцію можна записати у вигляді:

$$UC(X \mid Y) = -\sum_{i=1}^{n} p(x_i) \sum_{i=1}^{m} p(y_j \mid x_i) \log p(y_j \mid x_i).$$

Виходячи з уявлень про величини ентропії, що визначаються на підставі використання уявлень про можливості істинності тих чи інших повідомлень, що впливають на прийняття оптимальних рішень про модифікацію нейронних мереж, можна записати:

$$UC(Y \mid X) = UC(Y) - T(X, Y),$$

де

$$T(X, Y) = UC(X) + UC(Y) - UC(X, Y)$$
$$UC(X, Y) = -\sum_{i=1}^{n} \sum_{j=1}^{m} p(x_i, y_j) \log p(x_i, y_j),$$

де пари $(x_i y_j)$ являють собою елементи матриці витвори множин $X \times Y$. Відповідно до діаграмами Венна [16], $T(X, Y)$ являє собою перетин $UC(X)$ і $UC(Y \mid X)$.

Очевидним, при ухваленні рішення про модифікацію фрагментів нейронної мережі, є використання статистичних даних про раніше проведених адаптаційних модифікаціях. Для цього використовуються в більшості випадків механізми статистичних оцінок [17]. Однією з найпростіших оцінок є оцінка, яка представляє собою дисперсію, яка описується співвідношенням:

$$V = \sigma^2 = 1/N \sum_{i=-1}^{-N} [R_i^* - R_N]^2.$$

Якщо, при обчисленні такої оцінки використовується модель двох факторна, то відповідна оцінка реалізується на основі уявлень про щільність ймовірності того, що прийняте рішення буде успішним. Прикладом співвідношення дозволяє визначити величину такої ймовірності може служити [10, 18]:

$$P = 1/[1 + (\sigma / R_N)^2]$$

або співвідношення

$$R_U = R_N[1 + (\sigma / R_N)^2].$$

Слід зазначити, що статистичні дані, які представлені вибіркою N впливають на рівень довіри до прийнятих рішень R. Завдання вибору розмірів вибірки N, при яких рівень довіри до прийнятих рішень буде перебувати на бажаному рівні, вирішується на основі використання нерівності Чебишева, яке дозволяє визначити величину кордонів довіри 2ε на основі даних про кількість елементів у вибірці N:

$$P_\gamma\{R_N - \varepsilon < R < R_N + \varepsilon\} \geq 1 - \sigma^2 / N\varepsilon^2.$$

Проблемами оцінок параметрів, на підставі яких приймається найбільш вигідне рішення про модифікацію нейронної мережі, займається теорія статистичних оцінок. Для ілюстрації способів використання можливостей такої теорії, розглянемо двопараметричну функцію розподілу $g(x|p)$, в якій x - випадкова змінна, яка приймаючи k значень, які відповідають успішним рішенням в n незалежних рішень з ймовірністю p в кожному з усіх можливих рішень. Тоді, можна записати співвідношення:

$$P_\gamma(x = k) = \binom{n}{k} p^K (1-p)^{n-k}.$$

Для оцінки параметра p, виходячи зі статистичних даних про (k, n) вводиться функція правдоподібності:

$$\log L(p|k,n) = \log \binom{n}{k} + k \log p + (n-k) \log (1-p).$$

Щоб отримати оцінку максимальної правдоподібності параметра p, необхідно визначити максимум функції $\log L(p|k,n)$.

Модифікація фрагментів нейронної мережі спрямована на її адаптацію, незалежно від того закладаються в неї механізми модифікації, все ж може призводити до виникнення негативних результатів, інтерпретація яких може складатися в зменшенні рівня захищеності системи доступу, реалізованої на основі використання нейронної мережі. Виникнення негативних результатів може обумовлюватися неординарністю поведінки клієнтів, непередбаченими критичними ситуаціями, які можуть виникати в навколишньому середовищі мережі, з якої можуть надходити запити на доступ, будь-якими технічними катаклізмами в мережі, які обумовлюються природними або іншими обставинами і т.д. Якщо взяти до уваги, що в даному випадку ми говоримо про безпеку яка захищає локальні мережі, яка може бути порушена внаслідок невиконання своїх функцій системою доступу, то необхідно враховувати і наведені вище причини порушень в системі доступу. Одним з підходів дозволяє розглянути ці аспекти функціонування системи доступу, є введення і дослідження функції марності, яка повинна описувати втрати, до яких можуть привести успішно реалізовані процеси несанкціонованого доступу завдяки виникненню перерахованих вище факторів.

Для оцінки очікуваних втрат і небезпек можна розглянути двох факторну функцію марності, яка описується співвідношенням:

$$D(X_l) = F[K_\gamma R_l X_l, K_\gamma S_l] = K_\gamma R_l S_l^{1-\beta l} X_l^{\beta l},$$

де $S_l = 1 + K_l(\sigma_l / R_l)$, $X_l = K_l / K_\gamma$, K_γ - резервні кошти забезпечують позитивний результат модифікації пов'язаної з адаптаційними змінами в фрагментах нейронної мережі, R_γ - очікувана одиниця втрат з моделлю двох точкового розкладання

$$R_{lu} = 1 - (K_l^* / K_l) > 0 \text{ з ймовірністю } P_l$$

І $R_{ld} = 0$ с ймовірністю $1 - P_l$, K_l - величина, яка описує розміри можливих втрат, які, при $X_l \le 1$ можуть компенсувати резервні засоби K_γ. Слід зазначити, що одиниця очікуваних втрат R_l відповідає негативною величиною одиниці

виграшу (R). Тому, індекс безпеки можна записати у вигляді наступного співвідношення:

$$S_l = 1 + K_l \sqrt{(1/P_l) - 1},$$

де $K_l = (S_l^* - 1)/\sqrt{(1/P_l) - 1}$, P_l^* - верхня межа втрат, або $P_l \le P_l^*$. Приймемо, що функція $D_i(X_{li})$ опукла, або $\beta_l > 1$. Тоді, марність можна записати у вигляді наступного співвідношення:

$$D(x_l) = k_\gamma (R_l / S_l^{\beta_l - 1})\, x_l^{\beta l}.$$

Для того, щоб визначити S_l^*, необхідно визначитися з величиною коефіцієнта β_l, який характеризує мотивацію прийняття рішень. Це можна здійснити аналогічно способу визначення коефіцієнта β для функції корисності. В цьому випадку, розглядається параметр C, який визначає величину компенсації втрат, при виникненні ситуації, при якій мало місце успішне несанкціоноване втручання. В рамках даного підходу, для протидії можливості несанкціонованого доступу, реалізуються превентивні заходи відповідно до деякої стратегії. Розглянемо два базові принципи, на підставі яких можна визначити величину β.

Першим принципом є принцип еквівалентності впевненості. Це означає, що марність, яка визначає величину втрати k_l розглядається як величина рівнозначна втрат величиною, при відсутності ризику. Беручи до уваги умова $D(X_l) = D_l(C/K_\gamma)$, де $X_l = K_l / K_\gamma$ можна записати наступні співвідношення:

$$C/K_l = [(R_{lz})^{1/\beta_1}] / S_l^{\gamma_1},\ \gamma_1 = 1 - 1/\beta_l.$$

Другим принципом є принцип мінімізації функції марності, яка пов'язана з розподілом значень параметрів, які використовуються для реалізації превентивних дій з метою звести до мінімуму ризик втрат. В результаті перетворень аналогічних тим, які проводилися, при визначенні коефіцієнта β для функції корисності, можна записати:

$$\beta_l = [1 + (\ln(C/K_l))/(\ln(g^*/(1-\beta^*))]^{-1}.$$

При цьому, можна визначити оптимальну стратегію розподілу значень параметра K_P, які використовуються для попереджувальних дій таким чином, щоб мінімізувати марність небезпеки і відповідних втрат. Якщо припустити, що для попереджувальних дій використовуються кошти, значення яких дорівнює K, то можна записати наступне співвідношення:

$$R_P = 1 - [K_l^*(K) / K_l^*(0)] = R_l C^{-\varepsilon K},$$

де параметр ε визначається співвідношенням $\varepsilon = -(1/k)\ln[(k_c - k_c^*(k)/(k_c - k_c^*(0)]$, і характеризує ефективність попереджувальних дій для запобігання втрат.

Розглянуті вище концепції використання функції корисності, яка інтерпретується як очікуваний виграш, який з'являється в результаті підвищення рівня безпеки SD, також функції марності, яка інтерпретується як оцінка величини втрат внаслідок реалізації успішного несанкціонованого доступу, обумовленого небезпеками, можуть використовуватися для оцінки дій або перетворень, в яких враховуються ефект корисності і ефект від втрат. В цьому випадку можна записати наступне співвідношення, для узагальненої функції корисності:

$$\Delta U\ (X) = U\ (X) - D\ (X) = P\ [R_U P S^{1-\beta} - [(1-P)/S_l^{\beta l-1})\ X^{\beta l}].$$

Розглянуті вище підходи оцінки поточного стану мережі та результатів адаптаційних перетворень не розглядалися з точки зору обліку тривалості періоду функціонування нейронної мережі, в якій відбуваються процеси адаптації. Проте, відомі підходи, які використовуються по відношенню до об'єктів, для яких характерне використання статистичного аналізу, що ґрунтується на уявленнях про тимчасові ряди, що описують поведінку відповідних об'єктів. В цьому випадку, виділяється ряд фаз, для кожної з яких визначаються характерні функції оцінок і особливості процесів адаптації. Виділення різних фаз обумовлюється тим, що протягом тривалого часу, за визначенням, не можуть відбуватися процеси, які за своєю природою були б неоднорідними.

5.4. Дослідження процесів адаптації в системах доступу, описуваних нейронними мережами

Процеси локального характеру і процеси, що відбуваються в системі в цілому повинні бути пов’язаними рамками, які визначаються наступними ознаками, що характеризують систему:

— зв’язок повинен реалізовуватися в рамках функціонування системи, які обумовлюються завданнями захисту доступу,

— такий зв’язок має існувати в рамках технологічних процесів функціонування, якими, в даному випадку, є процеси організації нейронної мережі,

— зв’язок повинен існувати між параметрами і оцінками, які характеризують, в першу чергу, процеси адаптації,

— між різними методами оцінки і відповідно, ініціації процесів адаптації повинен існувати зв’язок наступності між ними,

— повинен існувати зв’язок між інтерпретаціями розглянутих підходів до реалізації процесів адаптації, яка відображає і описує завдання доступу.

В рамках даного підходу, фрагмент нейронної мережі, який використовується для формування всієї мережі, відрізняється рядом особливостей від фрагментів традиційних мереж. Ці особливості полягають у наступному:

— класичний акумулятор, який є базовим елементом нейрона, має додаткові функціональні входи,

— крім суматора і вузла реалізує функцію активації, до складу нейрона входить блок оцінки критеріїв адаптації,

— до складу фрагмента нейронної мережі включається елемент збереження ознак історії розвитку відповідного фрагмента.

Виходячи з положення про те, що характерною особливістю окремого нейрона і нейронної мережі, в цілому, є простота реалізації окремих елементів мережі, то розглянемо способи реалізації додаткових компонент нейрона. Додаткові функціональні входи суматора не пов’язані із загальною класичною структурою нейрона, а забезпечують зв’язок елементів нейрона з додатковими функціональними блоками.

Блок оцінки критеріїв адаптації, згідно з реалізованим алгоритмом, орієнтований на один з можливих критеріїв ознаки адаптації і являє собою спеціалізований блок реалізації алгоритму аналізу критерію і визначення доцільності ініціації нового етапу адаптації відповідного фрагмента. Вхідними даними, для цього спеціалізованого блоку, є дані надходять з виходу функціонального блоку аналізу вхідних змінних, який в класичному випадку представляє собою акумулятор вхідних сигналів.

Блок збереження ознак історії розвитку адаптаційних процесів, в окремому фрагменті нейронної мережі, по суті, являє собою пам'ять, яка містить дані, що є описом ефектів адаптації. Ефект адаптації визначається, як деяка залежність функціональних сигналів, що надходять з блоку аналізу критеріїв адаптації і сигналів, які формуються на виході блоку суматора нейрона. Формально, ефект адаптації на i – тому процесі адаптації для j – того нейрона A_{ji}^{d} описується співвідношенням:

$$A_{ji}^{d} = \left(y_{i+1} - y_i\right) / x_{i+1}^{F}$$

де y_{i+1} - вихідний сигнал блоку суматора (BS) на $i+1$ – кроці функціонування j – того BS, який синхронізується ініціалізацією процесу адаптації суматора BS_i, яка здійснюється функціональним сигналом x_{i+1}^{F}. Обчислення A_{ji}^{d} здійснюється в блоці пам'яті нейрона $\left(BP_j\right)$. Функціональна схема фрагмента нейронної мережі приведена на рисунку 5.4.1.

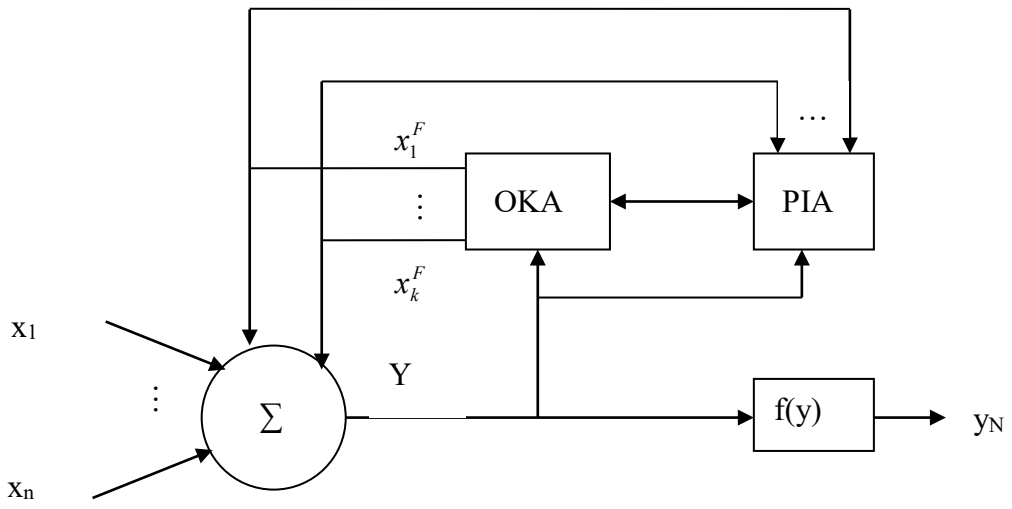


Рисунок 5.4.1 – Функціональна схема модифікованого елемента нейронної мережі.

На рисунку 5.1. прийняті наступні скорочення:

— $\sum$ – блок підсумовування вхідних параметрів або вхідних змінних $x_1,\cdots,x_k$.

— $f(y)$ – блок реалізації функції активації нейрона,

— OKA – блок оцінки критеріїв адаптації,

— PIA – блок запам'ятовування історії адаптації,

— $x_1,\cdots,x_k$. – функціональні змінні нейрона,

— y – внутрішня вихідна змінна.

Розглянемо більш детально процес функціонування одного фрагмента нейронної мережі, при реалізації процесу адаптації. Перш за все зазначимо, що реалізовувані процеси адаптації не впливають на функцію активації нейрона, яка є визначальною, для заданого типу нейрона. Це дозволить реалізовувати адаптацію таким чином, щоб остання не впливала або не приводила до зміни типу нейрона. Блоки OKA і PIA входять в роботу тільки в випадках, коли реалізується процедура адаптації. Питання про визначення моменту ініціалізації процесу адаптації, на даному етапі, розглядати не будемо. Приймемо також, що в рамках кожного фрагмента мережі, процеси вже відбувалися. Це означає, що в блоці PIA є дані про минулі процеси адаптації. Історичні дані представляють собою статистичні дані необхідні для розрахунку значень коефіцієнтів EU. Такими даними є значення y_i, які були отримані після i-го етапу реалізації процесу адаптації та ймовірності відповідного результату p_i. Завдяки використанню функції $U(x)$, вдається враховувати можливі нелінійності при розрахунку критерію EU.

У разі використання критерію $V(x,p_i,y,q)$, такими параметрами є ймовірності p_i і q, а також події x_i і y_i – які відображають значення на виході в разі, коли враховується можливий ризик, який пов'язаний з функціонуванням нейрона. При цьому ймовірності різних результатів замінюються функціями, які, по суті, повинні їх інтерполювати. Такі функції формуються виходячи з історичних даних з факторів що визначаються змінами функції перспективи $V(x,p_i,y,q)$. Аналогічна інформація формується в разі використання концепції $UC(x)$ або $UC(1/x)$.

У блоці OKA вирішуються такі завдання:

— завдання обчислення поточного значення величини критерію адаптації,

— завдання визначення необхідності переходу від одного критерію оцінки адаптації до іншого,

— завдання формування стратегії реалізації процесів адаптації.

Перше завдання вирішується шляхом обчислення величини критерію адаптації відповідно до алгоритму, який визначає відповідний критерій і являє собою незмінні процедури.

Друге завдання вирішується на основі аналізу зміни величини використаного критерію, до якого привели послідовно реалізовані процеси адаптації. Виходячи з інтерпретації використаних критеріїв таких, як величина корисності $U(x)$, величина перспективи $V(x, p_i, y, q)$, величина кількості інформації $UC(x)$, функції марності $D(x)$ і інших критеріїв, які допускають безпосередню інтерпретацію ефекту, до якого призводить реалізація процесу адаптації, в такий спосіб формується умова необхідності переходу від одного критерію до іншого. Нехай на деякому етапі функціонування використовуються критерії корисності EU. В цьому випадку, при повторенні процесу адаптації, значення функції корисності не повинно зменшуватися. Аналогічно переноситься інтерпретація критерію перспективи. Відповідне значення функції, для двох суміжних процесів адаптації не має зменшуватися. Таким же чином здійснюється перенесення інтерпретації інших критеріїв на процеси адаптації. Формально, ці переноси або проекції інтерпретації можна описати таким чином:

$$\delta_i \geq \left\{FK_j[A_i(s_i)] - FK_j[A_{i-1}(s_{i-1})\right\} \geq 0, \qquad (5.3)$$

де δ_i - позитивна константа, яка визначає допустиму межу коливань величини зміни відповідного критерію FK_j в результаті реалізації чергового процесу адаптації $A_i(s_i)$. Співвідношення (5.3) визначає стабілізуючу стратегію реалізації процесів адаптації. Відповідно до цієї стратегії, ініціалізація чергового процесу адаптації здійснюється наступним чином. Процес адаптації реалізується з інтервалом, який зростає до того моменту, коли $\Delta[FK_j(A_i(s_i))]$

змінюється в бік зменшення абсолютної величини $\Delta FK_j[A_i(s_i)]$ на величину перевершує δ_i. Формально, стратегія стабілізації, в кінцевому випадку, рівня безпеки доступу може бути описана співвідношенням:

$$\{0 > \Delta FK_j[A_i(s_i)] > \delta_i\} \to [\Delta T_{i+1} = (\Delta T_i - t_i)], \qquad (5.4)$$

де T_i - параметр визначає синхронізацію процесу ініціалізації адаптаційних перетворень в фрагменті s_i. Величина ΔT_i визначає поточний інтервал між черговими процесами адаптації. Слід зазначити, що параметр T_i не обов'язково є часом. У разі системи доступу, як синхронізуючий координати доцільно вибирати параметр, який характеризує кількість спроб несанкціонованого доступу. В цьому випадку, при збільшенні кількості таких спроб, доцільно припустити, що ймовірність виникнення вдалою або успішної спроби несанкціонованого доступу збільшиться. Тому, доцільно частіше проводити адаптацію нейронної мережі. Тоді, параметр ΔT являє собою кількість виявлених спроб несанкціонованого доступу протягом заданого інтервалу часу, що формально запишеться у вигляді співвідношення: $\Delta T_i = M / \tau$, де M - кількість спроб несанкціонованого доступу за період часу τ, який являє собою константу.

Мінлива t_i в співвідношенні (5.4) являє собою величину, яка визначається наступним співвідношенням: $t_i = \Delta M_i / \tau$, де ΔM_i - величина приросту кількості виявлених несанкціонованих звернень до системи, яка вибирається постійною. В цьому випадку, співвідношення для ΔT_i запишеться у вигляді наступного співвідношення:

$$\Delta T_i = (k \Delta M_i) / \tau .$$

Крім стабілізаційної стратегії (CS), може реалізовуватися прогресивна стратегія. Ця стратегія полягає в тому, що процеси адаптації повторюються відповідно до виконання наступної умови

$$\{[FK_j[A_i(s_i)] - FK_j[A_{i-1}(s_{i-1})]] \le \delta_i\} \to [\Delta T_{i+1} = \Delta T_i - t_i]. \qquad (5.5)$$

З наведеного співвідношення видно, що інтервал між черговими процесами адаптації зменшується, якщо величина різниці значення критеріїв двох чергових процесів зменшується і навпаки. В рамках прогресивної стратегії (PS) може мати місце ситуація, коли зменшення інтервалу ΔT_i не приводить до виконання умови (5.5), тоді реалізується стратегія зміни типу критеріїв адаптації (TS). Для реалізації стратегії TS, необхідно усі що використовуються критерії розподілити по рангу їх ефективності. Для більш конструктивного визначення ефективності критеріїв, розглянемо особливості реалізації процесів адаптації, які відповідають різним критеріям модифікації нейрона. Оскільки, основним механізмом модифікації є вплив OKA на елемент $\sum$, то модифікація нейрона може складатися в наступних діях з боку OKA:

— зміна кількості функціональних змінних, які подаються на вхід елемента підсумовування $\sum$;

— зміна величини вхідних сигналів x_i^F;

— комбінування кількості x_i^F, які трапляються на $\sum$ з величинами значень відповідних сигналів x_i^F, які залишаються незмінними протягом усього періоду функціонування нейрона починаючи від моменту адаптаційної модифікації, до моменту ініціації чергового процесу адаптації.

Очевидно, що інтерпретація відповідних дій повинна узгоджуватися з інтерпретацією алгоритмів, які відповідають різними критеріями оцінки величини адаптації. Тому, на прикладах розглянутих критеріїв корисності EU, критеріїв перспективи $V(x,p,y,q)$, інформаційного критерію $UC(Y \mid X)$ або $UC(X)$ і критерію марності $D(X)$, розглянемо інтерпретаційний зв'язок між x_i^F і параметрами критеріїв, а також між y_i і параметрами критеріїв. Величини критеріїв адаптації використовуються для реалізації різних стратегій реалізації процесів адаптації та безпосередньо в якості керуючого впливу на нейрон не використовуються. Параметри x_i^F інтерпретуються як параметри, які відображають вплив на фрагменти нейронної мережі. Найпростішим випадком є використання критерію

EU. При цьому $x_1,\ldots,x_n$ являють собою нормовані впливи на вхід нейрона або відповідають $x_1^F,\ldots,x_n^F$, а ймовірності фіналів стану нейрона $p_1,\ldots,p_k$ відповідає послідовність значень $y_1,\ldots,y_k$, які реалізуються на кожному етапі функціонування нейрона, яке відбувається між двома послідовними процесами адаптації. Імовірнісний характер змінних $y_1,\ldots,y_k$ забезпечує участь у формуванні вихідного сигналу y_i вхідних сигналів $x_1,\ldots,x_n$, які відображають змінні, використовувані в нейронній мережі для вирішення задачі захисту доступу. Прикладом таких змінних можуть служити:

— окремі параметри користувачів, які складають профіль користувача;

— параметри, які безпосередньо відображають рівень безпеки, який забезпечується засобами захисту, наприклад, кількість виявлених несанкціонованих спроб доступу, кількість виявлених атак на SD, оскільки атаки можуть складатися в дискредитації системи доступу тощо;

— нерегламентовані події, які виникають в процесі функціонування системи доступу що характеризуються відповідними параметрами і інші параметри, які безпосередньо чи опосередковано впливають на рівень безпеки, який забезпечують засоби захисту.

У разі використання критеріїв адаптації типу $V(x,p,y,q)$ змінні x_i інтерпретуються, як функціональні змінні x_i^F, які по суті представляють собою модифікуючий вплив, внаслідок якого відбувається адаптація нейрона. Значення змінної x_i^F, в цьому випадку, відображає величину функцій $\pi(x_i^F)$ і $\vartheta(x_j^F)$. Змінна y_i відповідає змінної y_i яка подається в блоки OKA і PIA. При цьому, величина зчитувальних значень y_i використовується для формування і корекції функції $\vartheta(Y)$ і, відповідно, для корекції функції $\vartheta(x)$. Таким чином, значення x_i^F може формуватися не тільки в результаті обліку значення величини критерію, а й з урахуванням величини змінних y_i. У разі використання критерію $UC(Y(X))$, кількість інформації не має безпосереднього прямого інтерпретаційного відображення на функціональні змінні x_i^F. Тому,

x_i^F використовувані для модифікації, формуються в результаті зворотних перетворень показників UC. Аналітичні залежності, в даному випадку, не формуються, а необхідні значення x_i^F обчислюються шляхом реалізації ітераційних процедур модифікації значень x_i, які є змінними, при обчисленні UC. Така ітераційна процедура триває до тих пір, поки UC не зміниться на величину ΔUC яка визначається умовою реалізації обраної стратегії. При цьому, ймовірність $p(x)$ і $p(y_i \mid x)$ обчислюється на підставі історичних даних про величини x_i і y_i які зберігаються в блоці PIA.

Критерій марності $D(X)$, з точки зору його інтерпретації і, відповідно, алгоритмічної реалізації є декілька специфічним і його використання доцільне в тих випадках, коли не вдається відповідно до стратегій CS, PS і стратегії, яка пов'язана з використанням інформаційних критеріїв (IS) проводити модифікацію нейронів. Ця ситуація, в рамках даного підходу відповідає випадку, коли в SD відбувається зниження рівня безпеки системи. В цьому випадку, стоїть завдання недопущення подальшого зниження рівня безпеки SD і використання критерію $D(X)$ є доцільним. Очевидно, що цей критерій використовується як засіб тимчасовий, якщо проводити деякі радикальні заходи по відновленню рівня безпеки немає можливості. Тому, можна встановити наступну ієрархію використання критеріїв адаптації, яка описується співвідношенням:

$$EU \rightarrow V(X,p,Y,q) \rightarrow UC(Y \mid X) \rightarrow D(X).$$

Відповідно до цього співвідношенням, залишається завдання прийняття рішення по ініціалізації процесів адаптації в разі, коли критерію $D(X)$ не достатньо, щоб задовольнити умовам стратегії, в рамках якої він використовується. Слід зазначити, що критерій $D(X)$ використовується виключно в рамках стратегії PS. Критерій $UC(Y \mid X)$ і критерії EU і $V(x,p,y,q)$ можуть використовуватися відповідно до стратегій CS і PS.

У разі невиконання умов стратегії PS при використанні $D(X)$ існують такі можливості вирішення виниклої проблеми:

— перехід до методів вирішення завдань визначення виникнення критичних ситуацій в SD;

— ініціативний перехід до критеріїв EU, $V(x, p, y, q)$ або $UC(Y \mid X)$ з власними умовами вибору одного з цих критеріїв.

5.5. Висновки до п'ятого розділу

У п'ятому розділі розглянуті основні способи реалізації процесів адаптації, при вирішенні завдань захисту систем доступу.

Визначено що процесом адаптації в системі SD є процес, який регламентується наступними співвідношеннями: процес адаптації може виробляти зміни оцінки значень аналізованих параметрів; процес адаптації не здійснює зміни логіки алгоритмів аналізу контрольованих параметрів; процес адаптації може змінювати кількість аналізованих параметрів, якщо це не призводить до змін логіки аналізу окремих параметрів.

Розглянуто ряд умов, які повинні виконуватися для того, щоб могли реалізовуватися дії в SD, класифікуються як дії процесів адаптації.

Визначено і проаналізовано аспекти, які є загальними для системи що володіє властивостями адаптації: визначення мети процесів адаптації; визначення тривалість процесів адаптації; визначення можливості методів адаптації в рішенні задач забезпечення безпеки SD, при змінних факторах, які ініціюють або пов'язані з процесами адаптації.

Обґрунтовано необхідність формування в рамках нейронної мережі спеціалізованих вузлів реалізують функції: ініціації процесів адаптації; контролю часу функціонування; аналізу умов завершення локального процесу адаптації; зв'язку фрагментів локальних процесів адаптації з інтегральними умовами узагальненого процесу адаптації в рамках всієї системи SD.

Запропоновано структуру фрагмента нейронної мережі, який використовується для формування всієї мережі, відрізняється рядом особливостей від фрагментів традиційних мереж. Ці особливості полягають у наступному:

— класичний акумулятор, який є базовим елементом нейрона, має додаткові функціональні входи;

— крім суматора і вузла реалізує функцію активації, до складу нейрона входить блок оцінки критеріїв адаптації;

— до складу фрагмента нейронної мережі включається елемент збереження ознак історії розвитку відповідного фрагмента.

Виходячи з положення про те, що характерною особливістю окремого нейрона і нейронної мережі, в цілому, є простота реалізації окремих елементів мережі, запропоновані способи реалізації додаткових компонент нейрона. Додаткові функціональні входи суматора не пов’язані із загальною класичною структурою нейрона, а забезпечують зв’язок елементів нейрона з додатковими функціональними блоками.

Блок оцінки критеріїв адаптації, згідно з реалізованим алгоритмом, орієнтований на один з можливих критеріїв ознаки адаптації і являє собою спеціалізований блок реалізації алгоритму аналізу критерію і визначення доцільності ініціації нового етапу адаптації відповідного фрагмента. Вхідними даними, для цього спеціалізованого блоку, є дані надходять з виходу функціонального блоку аналізу вхідних змінних, який в класичному випадку представляє собою акумулятор вхідних сигналів.

Блок збереження ознак історії розвитку адаптаційних процесів, в окремому фрагменті нейронної мережі, по суті, являє собою пам’ять, яка містить дані, що є описом ефектів адаптації. Ефект адаптації визначається, як деяка залежність функціональних сигналів, що надходять з блоку аналізу критеріїв адаптації і сигналів, які формуються на виході блоку суматора нейрона.

Розроблено функціональну схему фрагмента нейронної мережі.

Список використаних джерел до п’ятого розділу

1. В. В. Ященко, Н. П. Варновский, Ю. В. Нестеренко и др., *Введение в криптографию. 3-е Изд., доп.* Под ред. В.В. Ященко, М.: МЦНМО, 2000, С. 288.

2. В. Жельников, *Криптография от папируса до компьютера*, М.: ABF, 1996, С. 336.

3. А.А. Молдовян, Н.А. Молдовян, Б.Я. Советов, *Криптография. Серия «Учебники для вузов. Специальная литература»*, СПб.: «Лань», 2000, С. 224.

4. А.А. Петров, *Компьютерная безопасность. Криптографические методы защиты*, М.: ДМК, 2000, С. 448.

5. Фейт Сидни, *TCP/IP. Архитектура, протоколы, реализация (включая IP версии 6 и IP Security)*, М.: «Лори», 2000, С. 424.

6. Устинов Г. Н. Основы информационной безопасности систем и сетей передачи данных : Учебное пособие / Г.Н. Устинов. – М.: СИНТЕГ, 2000. – 248 с. – (Серия «Безопасность»).

7. Матфик С. Механизмы защиты в сетях ЭВМ / С. Матфик ; пер. с англ. – М.: Мир, 1993. – 216с.

8. Стенг Д. Секреты безопасности сетей / Д. Стенг, С. Мун. – К.: „Диалектика”, 1995. – 544 с.

9. Быков В. В. Цифровое моделирование в статистической радиотехнике / В.В. Быков. – М.: Сов. радио, 1971. – 326 с.

10. Лоэв М. Теория вероятностей / М. Лоэв ; пер. с фр. – М.: Изд-во иностранной литературы, 1962. – 720 с.

11. Ермаков С. М. Статистическое моделирование / С.М. Ермаков, Г.А. Михайлов. – М.: Наука, 1982. – 320 с.

12. Залыгин А. С. Прикладные методы статистического моделирования / А.С. Залыгин, Ю.И. Палагин. – Л.: Машиностроение, 1986. – 320 с.

13. Корченко А. Г. Несанкционированный доступ к компьютерным системам и методы защиты: учебное пособие / А.Г. Корченко. – К.: КМУГА, 1998. – 116 с.

14. Мелихов А. Н. Расплывчатые ситуационные модели принятия решений: учебн. пособие / Мелихов А. Н., Берштейн Л. С., Коровин С. Я. – Таганрог: ТРТИ, 1986. – 92 с.

15. Быховский М. А. Пионеры информационного века. История развития теории связи / М.А. Быховский. – М.: ЗАО «РИЦ «Техносфера», 2006. – 376 с. – (Серия «История электросвязи и радиотехники»).

16. Метод статистических испытаний / [Бусленко М.П., Голенко Д.И., Соболь И.М., Саргович В.Г., Шнейдер Ю.А.] .– М.: Физматиздат, 1962. – 280 с.

17. Бендат Дж Прикладной анализ случайных данных / Дж. Бендат, А. Пирсол. – М.: Мир, 1989. – 540 с.

18. Марченко Б.Г. Метод статистических интегральных представлений и его приложения в радиотехнике / Б.Г. Марченко . – К.: Наукова думка, 1973. – 191 с.

РОЗДІЛ 6. АПРОБАЦІЯ МЕТОДІВ ТА МОДЕЛЕЙ РОЗМЕЖУВАННЯ ДОСТУПУ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ

На основі запропонованих в роботі методів та моделей розмежування доступу до інформаційних ресурсів на протязі 2000-2020 років було проведено низку досліджень, які довели їх користь та адекватність. Роботи виконувались відповідно до плану науково-дослідних робіт Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України в рамках наступних науково-дослідних тем: НДР «Кріт» «Розробка методів побудови та формального опису критеріїв оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» № 0101U006700 (2001р.-2004р.). НДР «МодА» «Дослідження і розробка методів розпізнавання, які базуються на використанні спектральних перетворень, для інформаційного забезпечення безпеки енергетичних об'єктів» № 0105U001296 (2005р.-2008р.). НДР «Управление» «Розробка методів і комп'ютерних засобів підтримки прийняття рішень в задачах ситуаційного і технологічного управління в енергетиці» № 0102U005589 (2002р.-2006р.). НДР «Модель» «Розвиток теорії, розробка нових методів і засобів математичного й комп'ютерного моделювання енергетичних і енергоємних об'єктів, систем і установок» № 0107U001945 (2007р.-2009р.). НДР «МодБ» «Исследование и разработка методов повышения безопасности и эффективности распределенных высокопроизводительных информационных технологий при решении задач энергетики» №0108U010588 (2009р.-2013р.). НДР «МодД» «Дослідження та розробка методів оцінювання захищеності інформації в розподілених високопродуктивних інформаційних системах при вирішенні задач енергетики» № 0114U002361 (2014р.-2018р.). НДР «МодЕ» «Дослідження ризиків інформаційної безпеки об'єктів критичної інфраструктури ГТС України та розробка методології поводження з ними» № 0118U002371 (2019р.-по теперішній час). НДР «ГІБРИД» «Розвиток теорії, розробка методів та засобів реалізації гібридних експертно-моделюючих комп'ютерних систем в задачах комплексного управління перетворенням енергії» № 0112U000050

(2012р.-2016р.). НДР «НОВІНТЕХ» «Розвиток теорії, розробка новітніх інформаційних технологій в задачах комплексного моделювання та управління процесами перетворення та використання енергії» №0117U004347 (2017р.-по теперішній час). НДР «ГРІДІПМЕМОН-11» «Створення грід-системи моніторингу, збору та аналізу даних в енергетичній галузі на базі грід-центру з питань енергетики» №0111U004339 (2011р.-2013р.), згідно Державної цільової науково-технічної програми впровадження і застосування грід-технологій на 2009-2013 роки. НДР «ГРІДІПМЕМОН-15» «Підтримка та розвиток грід-сайту Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАНУ, як ресурсного центра NGI_UA, та створення грід-сервіса централізованого синтезу конфігурацій для апаратних прискорювачів задач інформаційної безпеки в енергетичній галузі» №0115U002876 (2015р.), згідно Цільової комплексної програми наукових досліджень НАН України «Грід-інфраструктура і грід-технології для наукових і науково-прикладних застосувань». НДР «ГРІДІПМЕМОН-16» «Підтримка та розвиток грід-сайту Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАНУ та створення системи централізованого програмування реконфігуровних прискорювачів задач інформаційної безпеки в енергетичній галузі» №0116U006907 (2016р.), згідно Цільової комплексної програми наукових досліджень НАН України «Грід-інфраструктура і грід-технології для наукових і науково-прикладних застосувань». НДР «ГРІДІПМЕМОН-18» «Підтримка грід-сайту Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАНУ та використання хмарної інфраструктури для централізованого програмування реконфігуровних засобів інформаційної безпеки в енергетичній галузі» №0118U001370 (2018р.), згідно Цільової комплексної програми наукових досліджень НАН України «Грід-інфраструктура і грід-технології для наукових і науково-прикладних застосувань». НДР «ГРІДІПМЕМОН-19» «Підтримка грід-сайту ІПМЕ ім. Г.Є. Пухова НАН України та модернізація веб-сервісу централізованого програмування реконфігуровних засобів інформаційної безпеки на базі гріду та хмарної інфраструктури» №0119U001812 (2019р.), згідно Програми інформатизації НАН України на 2019р. НДР «ГРІДІПМЕМОН-20»

«Підтримка грід-сайту ІПМЕ ім. Г.Є. Пухова НАН України та проведення експериментів з системою програмування реконфігуровних засобів на базі гріду та хмарної інфраструктури» №0120U103624 (2020 р.), згідно Програми інформатизації НАН України на 2020 р. Більшість з перерахованих НДР було виконано мною в якості наукового керівника, інші – в якості відповідального виконавця. Наведемо деякі результати цих робіт з метою ілюстрування ефективності розроблених моделей.

6.1. Експериментальне дослідження дворівневої моделі розмежування доступу до інформаційних ресурсів з обмеженим доступом

Прикладом реалізації алгоритмів розмежування доступу є реалізація алгоритму надання повноважень [1] (ANP) якій реалізує всі операції, необхідні, для реалізації процесу доступу до конфіденційних даних. Розглянемо докладніше проблеми які при цьому виникають. 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 $D_w^z = [(x_i^z), \ldots, j(x_{ik}^z)]$. Система SNP містить, крім самих даних, не тільки їх значення, а й інтерпретаційні описи цих даних $D_i^s = [j(x_1^s), \ldots, j(x_m^s)]$ [1]. 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. Для нас найбільш цікаво розподілені дані тому будемо розглядати дані представлені N- мерним масивом R_i^{kt} .

До таких параметрів відносяться наступні параметри даних:

– рівень конфіденційності даних $R_i^{kt}(x_i)$;

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

– рівень обгрунтованості 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 $\aleph_i\left(x_i^s\right)$ в процесі функціонування *IS* змінюється, оскільки він визначається частотою його використання на заданому інтервалі часу ΔT. Рівень відмінності між $\aleph_i\left(x_i^z\right)$ та $\aleph_i\left(x_i^s\right)$ 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 $R_i^{kt}[x_i(x_i^z)]$ задачею Za_i, які розміщаються в описі мети розв'язання задачі $C(Za_i)$ [2]. Маємо зауважити що складність перевірки параметру $R_i^{kt}[x_i(x_i^z)]$ зростає в квадратичному порядку в порівнянні с векторнім варіантом.

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 $R_i^t(x_i^z) \sqsubset R_i^t(x_i^s)$, де знак $\sqsubset$ – означає нижчий діапазон значень конфіденційності даних. Після цього *SNP* перевіряє, чи $C_i[Z_{ai}(R_i^{*t}(x_i))]$ відповідає меті, яка задана у параметрах задачі. Якщо така відповідність існує, то задача отримує по цьому параметру дозвіл на використання даних, у яких$[R_i^t(x_i)\&(k \sqsubset m)]$, 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 [3].

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 $\{r^t, \aleph_i, \lambda_i\}$ [4].

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 $I(D_w) = j(x_s^w),\ldots, j(x_m^w)$ по відношенню до $I(D_v) = j(x_i^v),\ldots, j(x_k^v)$. 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 $R_t(Z_{ai})$. 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 свого 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 [5] прикладом

якої може служити модель, що використовує генетичні алгоритми [6, 7]. За своєю природою *IS* є базою даних і, тому вводити в *IS* алгоритми типу генетичних не достатньо коректне.

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 [8-13]. 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 прокласти шлях суб'єкту з області *A* в область *C*. При цьому суб'єкт не повинен наближатися до об'єкту на відстань *D* для попередження розголошення конфіденційної інформації про об'єкт з області *B*. Класична модель доступу вирішує цю проблему за рахунок обходу області *B* межею. Використовуючи дворівневу модель доступу до даних, можна побудувати критерій нерозголошення конфіденційної інформації. Наприклад, дозволити рух об'єкта в області *B* та аналізуючи траєкторію його руху, з метою не допущення його попадання в деяку область контакту об'єктів із 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 нерозголошення 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. Відображаються 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 прийматися 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 [14-16] 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 цільовим призначенням є знаходження довжини.

Таким чином, для проведення експерименту необхідно запустити «pathfindermodel.exe». У меню (див. рис. 6.1.1) необхідно задати параметри моделювання і відкрити карту (див. рис. 6.1.2).

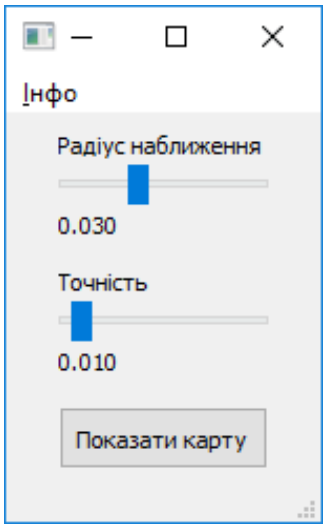


Рисунок 6.1.1 – Меню вибору параметрів

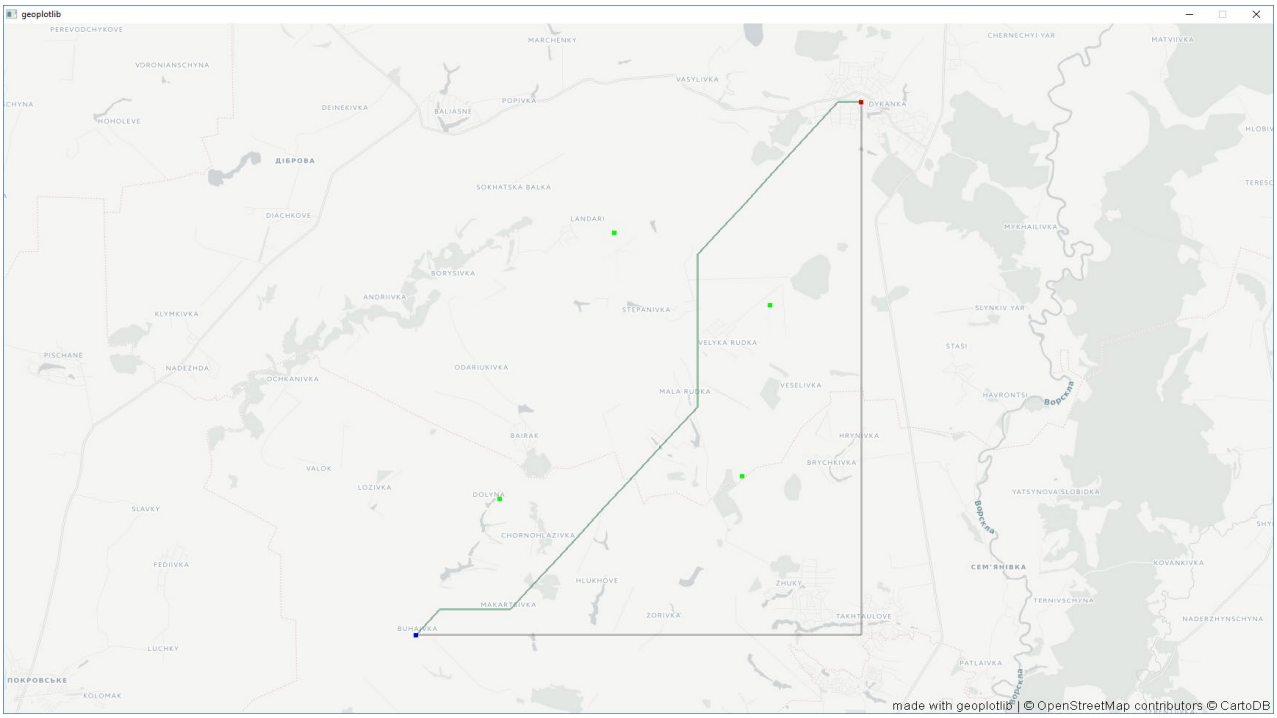


Рисунок 6.1.2 – Результати одиничного розрахунку

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. Математичне сподівання частки шляху становить 0,8025. Тобто середній виграш від застосування дворівневої моделі доступу до даних, при 1000 експериментах становить 19,75% від максимального шляху [8-13].

Характер кривої нагадує нормальний розподіл. Для уточнення побудуємо поверхню, яка показує результати більшого числа експериментів. У таблиці 6.1 наведено розподіл кількості результатів при фіксованих D і H для різного числа експериментів.

Таблиця 6.1

Розподіл кількості результатів для різного числа експериментів

Радіус наближення D	Точність розрахунку 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 6.1.3 приведено графічні результати проведених експериментів при зростанні їх числа. Аналізуючи отриману поверхню видно, що із збільшенням

кількості 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.

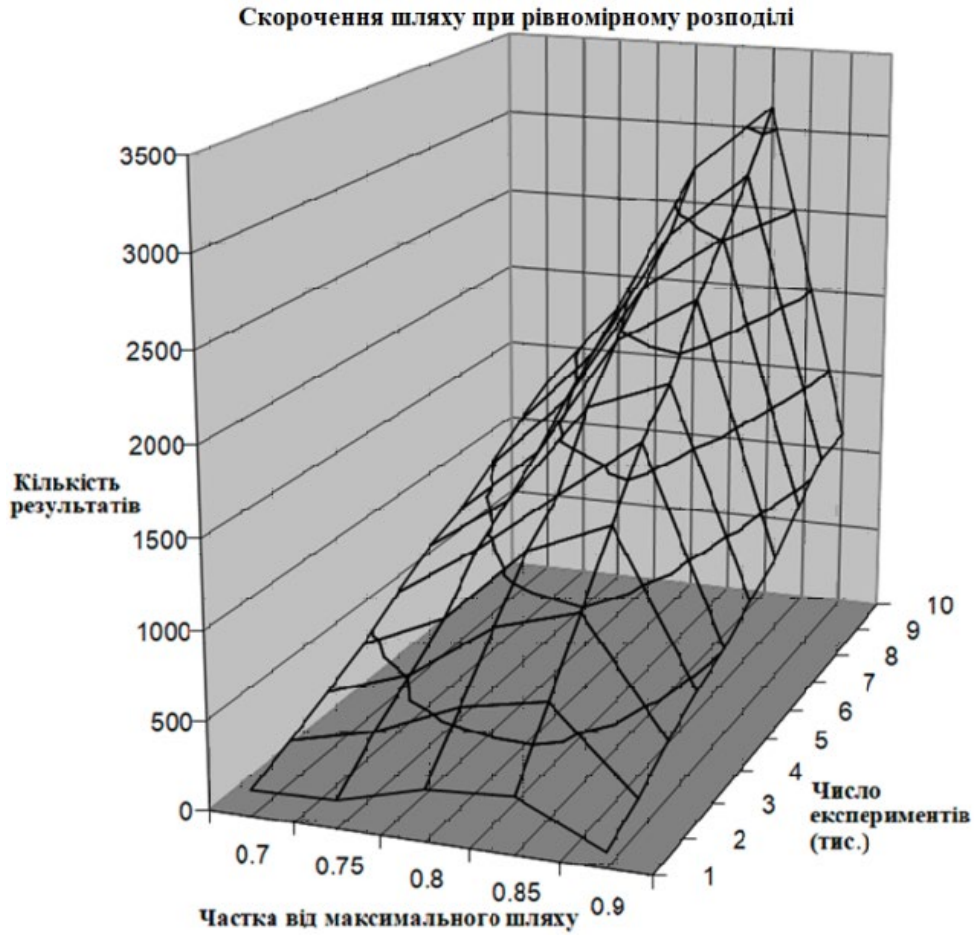


Рисунок 6.1.3 – Результати експериментальних

6.2.Системи біометричної автентифікації користувачів інформаційних систем за їх клавіатурним та рукописним почерком

Невід'ємною складовою процесу розмежування доступу до ресурсів будь-якої системи є автентифікація користувачів цієї системи. Для вирішення цієї задачі були створенні дві системи біометричної автентифікації користувачів інформаційних систем, за клавіатурним та за рукописним почерком відповідно, після чого було досліджено доцільність їх застосування.

Дані системи працюють в трьох режимах:

1. Налаштування системи, при якій виконується налаштування параметрів системи, відповідно до умов її використання.

2. Первісна реєстрація, при якій створюється база даних навчальних зразків відповідних біометричних характеристик необхідної кількості для кожного користувача.

3. Автентифікація, при якій спочатку вводиться ім'я користувача і потім, якщо в базі даних є навчальні зразки для цього користувача, створюється зразок біометричних характеристик даної людини і порівнюється зі зразками перевіряємого користувача, що зберігаються в базі даних. Результатом порівняння є число – імовірність того, що порівнювані зразки належать одній людині. Потім з використанням математичного критерію приймається рішення про ідентичність зразків, тобто вирішується, чи дійсно цей користувач той за кого себе видає.

Етап початкової реєстрації, в процесі роботи системи, необхідно повторити якщо:

1. Через якийсь час біометричні характеристики людини, що аналізуються, значно змінилися.

2. При початковій реєстрації, з якихось причин були зібрані неточні (помилкові) зразки, і внаслідок цього відбуваються часті відмови легальному користувачеві.

В якості механізму розпізнавання в даних системах використовується імовірнісна нейронна мережа (див. рис. 6.2.1), в якій в основу класифікації покладено використання методів Байеса.

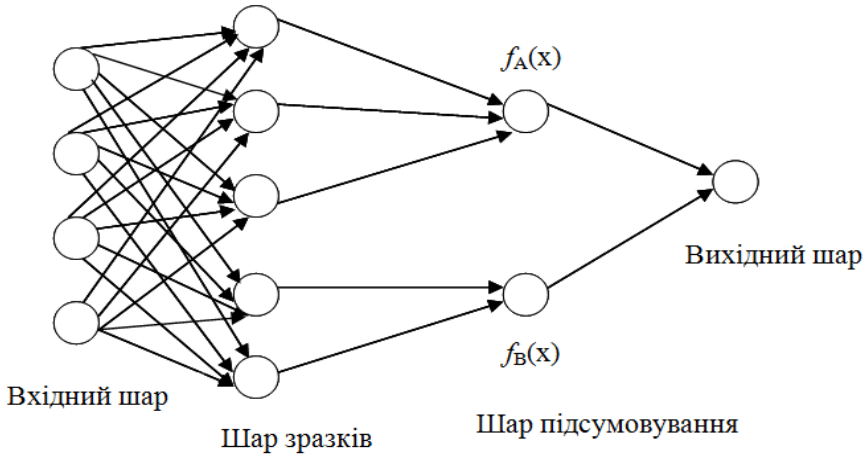


Рисунок 6.2.1 – Приклад архітектури імовірнісної нейронної мережі

Архітектура імовірнісної нейронної мережі складається з чотирьох шарів і визначається структурою навчальних даних:

— число вхідних елементів дорівнює числу ознак;

— число елементів шару зразків дорівнює числу навчальних зразків;

— число елементів шару підсумовування дорівнює числу класів;

— число елементів вихідного шару завжди дорівнює 1.

Система автентифікації користувачів за їх клавіатурним почерком

Система біометричної автентифікація «АКП» заснована на аналізі клавіатурного почерку користувачів інформаційної системи [17-22]. Дана система розроблена на мові C++ Builder з використанням, для обробки та зберігання інформації, програми Database Desktop та SQL-запитів. Програма працює під керуванням ОС Windows. Для формування та динамічного передавання характеристик клавіатурного почерку користувача в комп'ютер використовується клавіатура. В якості механізму розпізнавання використовується імовірнісна нейронна мережа.

Складовою частиною даної системи автентифікації є модулі реалізації первинної обробки зразків клавіатурного почерку (див. рис. 6.2.2.) [17-22].

Рисунок 6.2.2 – Первинна обробка зразків клавіатурного почерку

Первинна обробка зразків клавіатурного почерку складається з наступних двох частин і реалізується за допомогою відповідних модулів:

1. ВФХ – вибір ключової фрази та характеристик, що будуть аналізуватися під час автентифікації користувачів. Для цього виконується аналіз зразків з пробної бази даних навчальних зразків для вибору набору ключової фрази та символів ключової фрази, динаміка вводу яких буде аналізуватися під час автентифікації. Цей відбір реалізуються за допомогою наступних модулів:

— ВФ – вибір ключової фрази на основі аналізу накопичених зразків клавіатурного почерку з пробної бази даних, завдяки аналізу навчальних зразків введення різних наборів ключових фраз, за критеріями мінімуму амплітуди розподілу відсотка помилок у користувачів, під час вводу ключової фрази.

— ВХ – вибір характеристик, що будуть аналізуватися при автентифікації, а саме, за допомогою пошуку мінімуму значення спеціальної функції від математичного очікування та дисперсії, в ключовій фразі (обраній за допомогою модулю ВФ) обираються символи, динаміка вводу яких є характерною для групи користувачів.

2. ПВ – попередній відбір навчальних зразків, які будуть використовуватись для розпізнавання. Цей відбір полягає в видаленні з бази даних навчальних зразків тих зразків, в яких присутні грубі помилки, за допомогою порівняння кожної характеристики зразка з її середньоарифметичним значенням для відповідного користувача.

Робота системи автентифікації користувачів за їх клавіатурним почерком складається з десяти етапів і реалізується за допомогою наступних модулів (див. рис. 6.2.3) [17-22]:

1. АФ1 – попереднє формування множини ознак клавіатурного почерку користувача. Ознакою в даній системі є часовий інтервал між натисканням клавіш двох сусідніх символів ключової фрази.

2. АФ2 – налаштування параметрів, які є найбільш критичними при

автентифікації користувачів за їх клавіатурним почерком. В даній системі налаштовуються такі параметри: необхідна кількість навчальних зразків; кількість слів в наборі, динаміка вводу яких може аналізуватися; кількість символів, динаміка введення яких аналізується; значення коефіцієнту (*k*), який використовується при виконанні модуля ПВ первинної обробки зразків

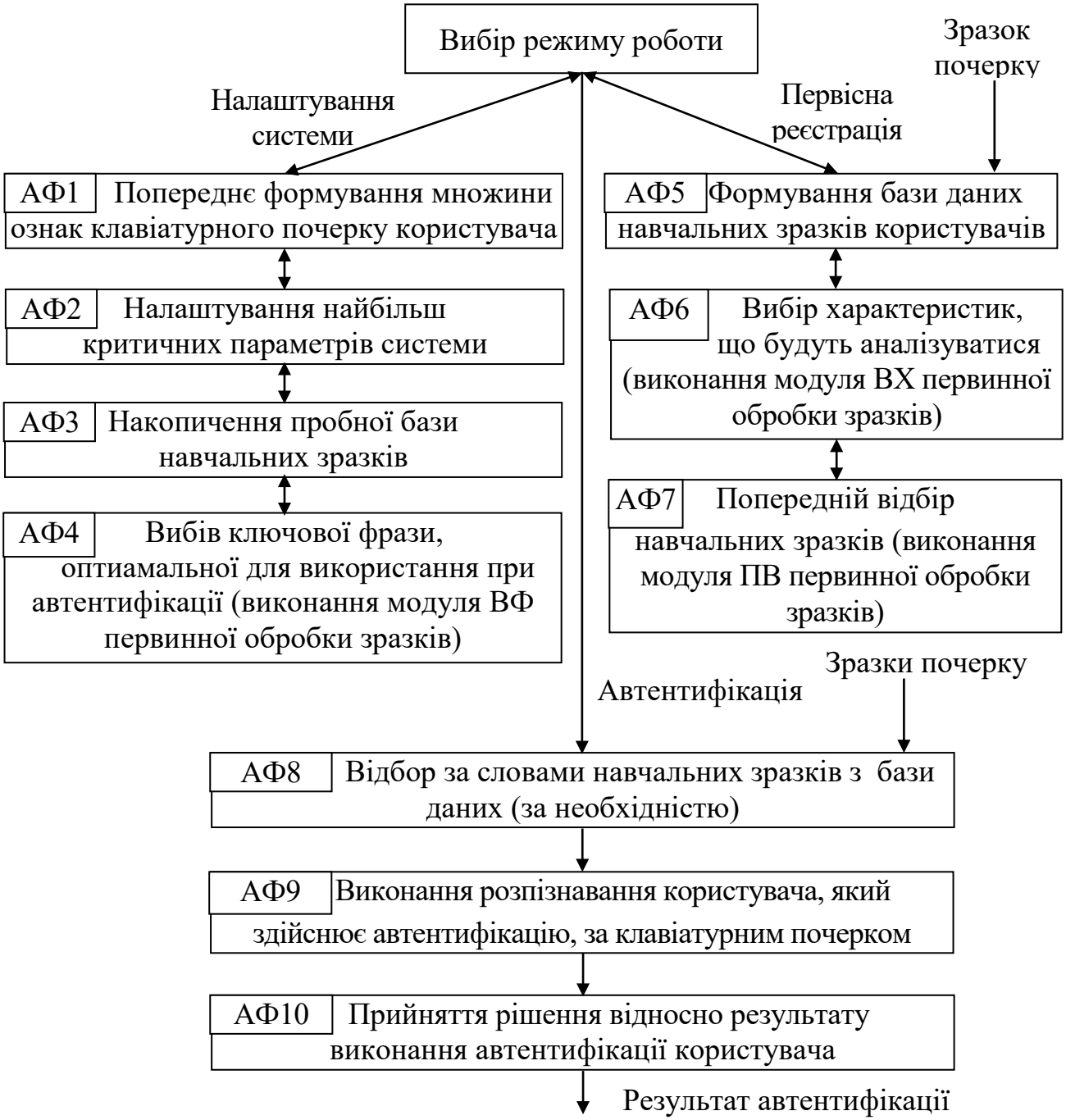


Рисунок 6.2.3 – Етапи роботи системи автентифікації користувачів за їх клавіатурним почерком

клавіатурного почерку.

3. АФ3 – накопичення пробної бази даних навчальних зразків для визначення (експериментально) оптимальної ключової фрази, динаміка вводу символів якої буде аналізуватися для автентифікації користувачів.

4. АФ4 – вибір ключової фрази, оптимальної для використання при автентифікації, на основі аналізу накопичених зразків клавіатурного почерку з пробної бази даних. Бажано обирати ті слова, які часто використовуються в роботі користувачів даної інформаційної системи, тому що динаміка саме їх вводу буде найбільш характерна. Крім цього це суттєво у випадку, якщо автентифікація виконується для проведення прихованого моніторингу. Для вибору виконується модуль ВФ первинної обробки зразків почерку.

5. АФ5 – формування бази даних навчальних зразків почерку користувачів необхідного об’єму для обраної ключової фрази (реєстрація користувачів в системі). Якщо користувач намагається виконати автентифікацію, а в базі даних недостатньо навчальних зразків його почерку, тоді його не допускають до автентифікації, а направляють на формування бази даних навчальних зразків.

6. АФ6 – вибір характеристик, що будуть аналізуватися при автентифікації, тобто вибір часові інтервали між вводом яких символів ключової фрази будуть аналізуватися при автентифікації. Для вибору виконується модуль ВХ первинної обробки зразків почерку.

7. АФ7 – попередній відбір навчальних зразків, які будуть використовуватись для розпізнавання. Тобто видалення з бази даних тих навчальних зразків, в яких присутнє суттєве відхиленням хоча б однієї з ознак. В даній системі під суттєвими відхиленням малося на увазі відхилення значення ознаки зразка від середньоарифметичного значення цієї ж ознаки у всіх інших навчальних зразках почерку цього користувача, на відсоток більший, ніж вказано в налаштуваннях системи розпізнавання. Для виконання цієї задачі виконуються модуль ПВ первинної обробки зразків почерку.

8. АФ8 – виконання, за необхідністю, відбору за словами навчальних зразків з бази даних. Якщо в системі налаштовано, що аналізується часові інтервали між введенням сусідніх символів не однакового фрагмента всіх слів набору, а часові інтервали між введенням сусідніх символів всього слова, тоді з множини навчальних зразків почерку обираються тільки зразки вводу того слова, яке вводить в даному сеансі автентифікації, користувач, що розпізнається.

9. АФ9 – виконання розпізнавання користувача, який здійснює автентифікацію, за клавіатурним почерком. Задачу розпізнавання користувачів, в даному випадку, можна звести до задачі класифікації образів. В якості механізму класифікації образів, в даній системі використовується імовірнісна нейронна мережа (див. рис. 6.2.1), архітектура, якої визначається відповідно до задачі розпізнавання динаміки вводу ключової фрази користувачів.

10. АФ10 – прийняття рішення відносно результату виконання автентифікації користувача інформаційної системи. Якщо на етапі АФ9 визначилось, що пред'явлений зразок почерку належить саме тому користувачу, що здійснює автентифікацію, тоді система автентифікації формує позитивний висновок відносно виконання автентифікації користувача інформаційної системи за його клавіатурним почерком.

Для збільшення імовірності правильного розпізнавання можна аналізувати наприклад, не тільки часові інтервали між натисканням двох сусідніх символів ключової фрази, а й часові інтервали між натисканням та відпусканням (або між відпусканнями) відповідних символів. Крім того, у всіх людей різний ступінь уваги, тому кількість зроблених помилок, частота їх повторювання і слова, при вводі яких виник збій – це досить індивідуальні характеристики, які теж можна використовувати при автентифікації.

Для визначення доцільності використання розробленої системи було проведено низку експериментів, основні результати яких продемонстровані на рисунку 6.2.4.

Дана система автентифікації користувачів за їх клавіатурним почерком дозволяє збільшити ступень багатофакторності автентифікації інформаційних систем не вимагаючи для цього додаткового обладнання.

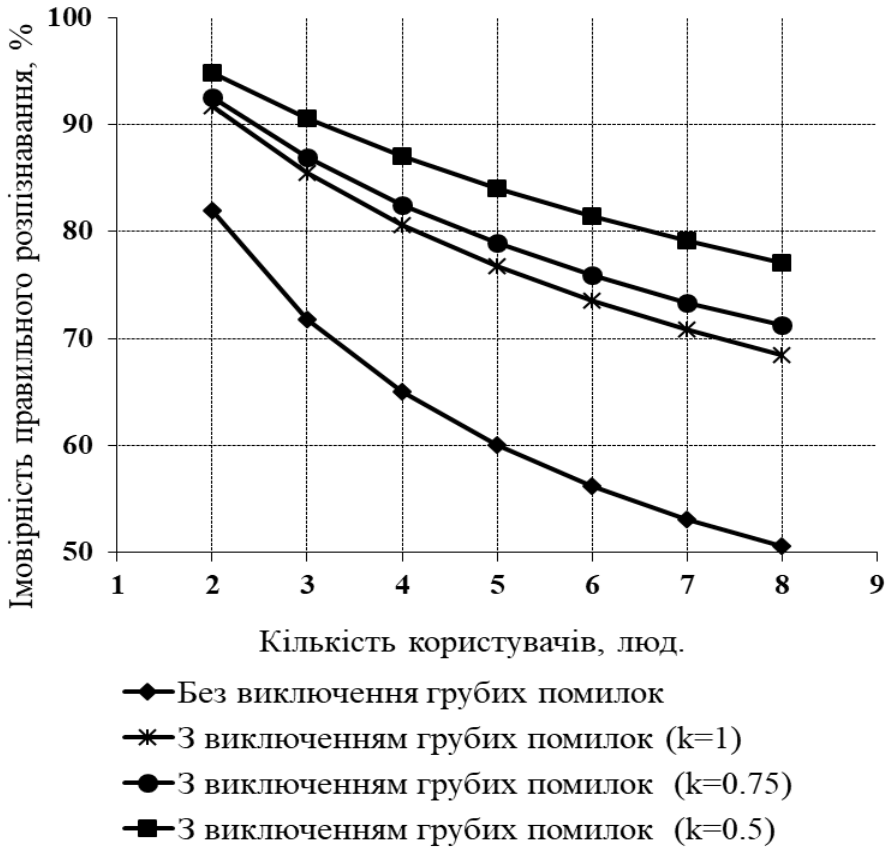


Рисунок 6.2.4 – Імовірність правильного розпізнавання користувачів інформаційних систем за їх клавіатурним почерком

Система автентифікації користувачів за їх рукописним почерком

Система біометричної автентифікація «АРП» заснована на аналізі рукописного почерку користувачів інформаційної системи [18, 20, 23-26]. Дана система розроблена на мові Delphi з використанням, для обробки та зберігання інформації, програми Database Desktop та SQL-запитів. Програма працює під керуванням ОС Windows. Як засіб формування та динамічного передавання характеристик рукописного почерку користувача в комп'ютер використовується графічний планшет, як один з варіантів пристрою з сенсорним екраном, враховуються характеристики графічного планшету; використовується інтерфейс для роботи з ним (Wintab) та єдина модель біометричних технологій розпізнавання (BioAPI). У зв'язку з цим в Delphi було додатково встановлено компонент JanHWinTab (сторінка Jan Hlavenka) – компонент для роботи с графічним планшетом (компонент використовує інтерфейс Wintab). В якості механізму розпізнавання використовується імовірнісна нейронна мережа.

Складовою частиною даної системи автентифікації є модулі реалізації первинної обробки зразків рукописного почерку (див. рис. 6.2.5.) [18, 20, 23-26]. Необхідність цієї обробки викликана специфікою використання графічного планшету та деякою нестабільністю, яка властива рукописному почерку. Імовірнісна нейронна мережа досить непогано справляється з цією проблемою, але якщо в зразку присутні дані, які є випадковими відхиленнями (помилками), які є несуттєвими для автентифікації і будуть тільки погіршувати якість розпізнавання, тоді їх необхідно або видалити або виправити (в залежності від типу помилки).

Рисунок 6.2.5 Первинна обробка зразків рукописного почерку

Первинна обробка зразків рукописного почерку складається з наступних двох частин і виконується на різних стадіях роботи системи автентифікації:

1. Попередній відбір даних, які будуть використовуватись для розпізнавання. Цей відбір полягає у видаленні помилок перших п’яти типів і реалізується за

допомогою наступних модулів:

— В1 – видалення помилок 1-го типу, а саме послідовностей точок з нульовим тиском (крім першої подібної точки з кожної послідовності). Виникають якщо користувач провів ручкою над графічним планшетом на невеликій відстані, не доторкнувшись до нього.

— В2 – видалення помилок 2-го типу, а саме випадкових точок (невеликої кількості). Виникають якщо користувач випадково доторкнеться ручкою до робочої області графічного планшету.

— В3 – видалення помилок 3-го типу, а саме повторів, тобто послідовностей точок, що йдуть підряд, в яких значення координат по обом осям не змінилися (крім випадку, коли у одній з точок нульовий тиск). Виникають якщо пакет даних передався в комп’ютер в зв’язку з зміною не координат по якоїсь з осей, а іншого параметру.

— В4 – видалення помилок 4-го типу, а саме випадкових невеликих загинів (частіше, з гострим кутом) на початку ліній. Виникають через тремтіння руки користувача або з вини інертності графічного планшету.

— В5 – видалення помилок 5-го типу, а саме неякісних зразків, які відкидаються через неможливість розбивки зображення ключової фрази на задану кількість зображень символів. Виникають якщо або вводиться неправильна ключова фраза, або якщо користувач має малий досвід роботи з графічним планшетом, або якщо користувач які-небудь символи написав не окремо, а разом.

2. Корекція даних, які будуть використовуватись для розпізнавання зразків рукописного почерку. Ця корекція полягає у виправленні помилок 6-8 типів, які викликані неправильним розміщенням написаної ключової фрази на робочій області графічного планшету і реалізується за допомогою наступних модулів:

— К1 – виправлення помилок 6-го типу, а саме різного кута нахилу, відносно осей робочої області графічного планшету, зображення ключової фрази у різних користувачів. Для виправлення таких помилок виконується

корекція 1-го типу, а саме посимвольний поворот зображень символів для нормалізації кута нахилу їх осей координат.

— К2 – виправлення помилок 7-го типу, а саме різного місця розташування на робочій області графічного планшету зображення ключової фрази у різних користувачів. Для виправлення таких помилок виконується корекція 2-го типу, а саме посимвольний зсув зображень кожного символу в центр робочої області обраного розміру.

— К3 – виправлення помилок 8-го типу, а саме різного розміру зображення ключової фрази, на робочій області графічного планшету, у різних користувачів. Для виправлення таких помилок виконується корекція 3-го типу, а саме посимвольне пропорційне масштабування (розтягування/стискання) зображень кожного символу на всю робочу область обраного розміру.

Робота системи автентифікації користувачів за їх рукописним почерком складається з одинадцяти етапів і реалізується за допомогою наступних модулів (див. рис. 6.2.6) [18, 20, 23-26]:

1. А1 – попереднє формування множини ознак рукописного почерку користувача. Ця множина складається з векторів ознак, значення яких передаються з графічного планшету (координати точок та тиск, з яким користувач натискає ручкою на сенсорний екран під час створення точок) та з векторів ознак, які обраховуються на наступних етапах роботи системи і є похідними від тих, що передані з графічного планшету. Також можуть аналізуватися вектори ознак не тільки точок зображення, а й параметри загальні для всього символу. Кількість ознак, що аналізуються, залежить від співвідношення надійності системи, яка вимагається, до припустимого об’єму ресурсів, що можуть бути задіяні.

2. А2 – налаштування параметрів, які є найбільш критичними при автентифікації користувачів за їх рукописним почерком. Цими параметрами є: необхідна кількість символів ключової фрази; мінімальна необхідна кількість зразків в базі даних навчальних зразків для кожного користувача; помилки яких типів необхідно видаляти і при яких умовах (довжина послідовності точок, які повинні вважатися випадковими та

довжина лінії до її загину, яка повинна вважатися помилкою); які типи корекції даних проводити перед розпізнаванням стилю написання ключової фрази; з яких типів точок формувати множину контрольних точок; довжина частини лінії, на якій треба обрати тільки одну контрольну точку 2-го типу.

3. А3 – формування бази даних навчальних зразків користувачів. В залежності від заданого режиму роботи, отриманий зразок почерку користувача, буде зареєстрований в базі даних навчальних зразків або відправлений на автентифікацію. Якщо накопичено недостатньо навчальних зразків для користувача, що розпізнається, тоді його не допускають до етапу автентифікації, а направляють на даний етап, тобто на формування бази даних навчальних зразків. Однією з особливостей принципу роботи графічного планшету, яка врахована в даній системі автентифікації, є той факт, що пакет даних з параметрами точки передається в комп'ютер, якщо змінилось значення хоча б одного параметру. Внаслідок цього в систему передаються зайві пакети даних (помилки 1-го типу), які видаляються за допомогою виконання модулю В1 первинної обробки зразків. Крім параметрів точок зображення ключової фрази та "логіна" користувача в даній системі фіксуються, дата та час створення точки. Необхідною умовою для роботи даної системи є те, що символи ключової фрази повинні бути написані не разом, а окремо один від одного.

4. А4 – видалення помилок 2,3,4 типів. Для виконання цієї задачі виконуються модулі В2, В3, В4 первинної обробки зразків.

5. А5 – умовне розділення зображення ключової фрази на зображення окремих символів. За рахунок виконання цього етапу досягається спрощення реалізації етапів А3, А8, А10 та значне зменшення об'єму ресурсів, що використовуються під час розпізнавання (за рахунок зменшення довжини зразка почерку). Якщо після розділення, кількість отриманих зображень виявляється менша, ніж кількість символів в ключовій фразі, тоді це помилка 5-го типу і для її видалення виконується модуль В5 первинної обробки зразків. Якщо навпаки, кількість отриманих зображень виявляється більша, ніж повинна бути, тобто деякі символи складаються з декількох частин, тоді ці частини з'єднуються.

6. А6 – корекція даних, які будуть використовуватись для розпізнавання зразків рукописного почерку. Для виконання цієї задачі виконуються модулі К1, К2, К3 первинної обробки зразків.

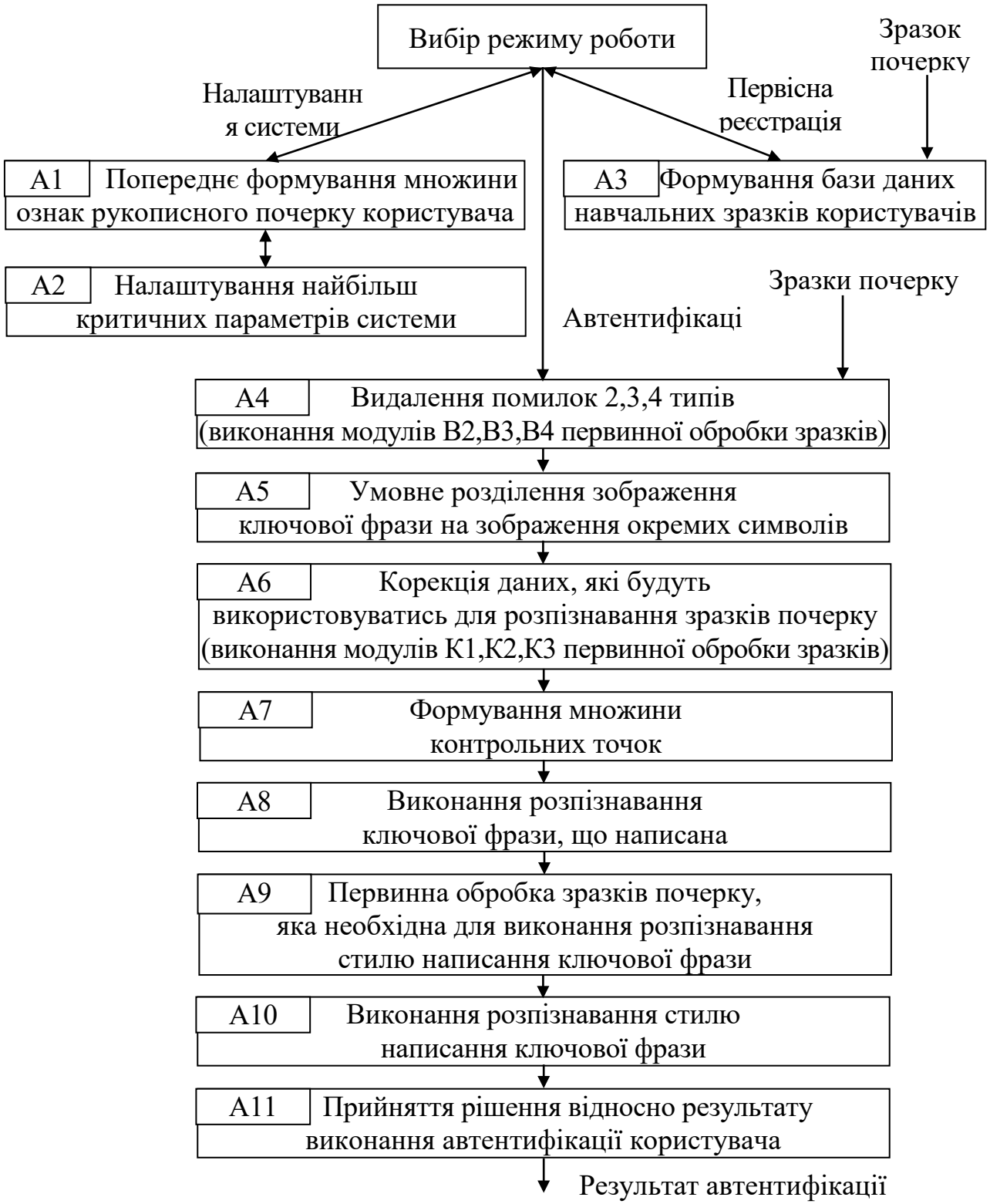


Рисунок 6.2.6 – Етапи роботи системи автентифікації користувачів за їх рукописним почерком

7. А7 – формування множини контрольних точок. За рахунок виконання цього етапу досягається спрощення реалізації етапів А8, А10 (значне зменшення об’єму ресурсів). В даній системі автентифікації аналізуються характеристики не всіх точок, а тільки найбільш значимих точок для кожного символу – контрольних точок наступних трьох типів:

— початкові та кінцеві точки кожної лінії, тобто точки торкання ручкою робочої області планшету та точки відриву ручки від планшету;

— кутові точки ліній, тобто точки, які знаходяться на вигині лінії;

— точки перетинання ліній, тобто точки, які знаходяться на перетинанні ліній.

При правильному розміщенні контрольних точок в кожному символі їх кількість буде приблизно однаковою, що є необхідною умовою для подальшого розпізнавання.

8. А8 – виконання розпізнавання ключової фрази, що написана. Задача розпізнавання образів, в даному випадку, зводиться до задачі класифікації образів. В якості механізму класифікації образів, в даному випадку, використовується імовірнісна нейронна мережа (див. рис. 6.2.1), архітектура якої обумовлена тим, що ця мережа повинна розпізнавати кожний написаний на графічному планшеті символ. Якщо всі символи розпізнані правильно, тоді приймається рушення, що написана правильна ключова фраза. В залежності від необхідного рівня безпеки, рішення про успішне розпізнавання можна приймати не обов’язково при правильному розпізнаванні всіх символів фрази, а наприклад, при розпізнаванні 5 з 6 символів.

9. А9 – первинна обробка зразків рукописного почерку користувачів, яка необхідна для виконання розпізнавання стилю написання ключової фрази. Які саме модулі первинної обробки зразків необхідно виконувати на цьому етапі визначається за допомогою експериментів в кожному конкретному випадку застосування даної системи автентифікації і налаштовуються на етапі А2.

10. А10 – виконання розпізнавання стилю написання ключової фрази. В даному випадку, як і на етапі А8, задача розпізнавання зводиться до задачі класифікації образів (користувачів). В залежності від вимог до системи, в якості параметрів, що

аналізуються, використовуються всі, або деякі ознаки множини ознак. Відповідно до цього і визначається архітектура імовірнісної нейронної мережі (див. рис. 6.2.1), яка використовується для розпізнавання стилю написання ключової фрази.

11. А11 – прийняття рішення відносно результату виконання автентифікації користувача інформаційної системи. Якщо на етапах А8 і А10 одержано позитивні результати, тоді система автентифікації формує позитивний висновок відносно виконання автентифікації користувача інформаційної системи.

Для визначення доцільності використання розробленої системи було проведено низку експериментів, основні результати яких продемонстровані на рисунку 6.2.7.

Дана система автентифікації користувачів за їх рукописним почерком дозволяє збільшити ступень багатофакторності автентифікації інформаційних систем при наявності стандартних сенсорних засобів вводу графічної інформації.

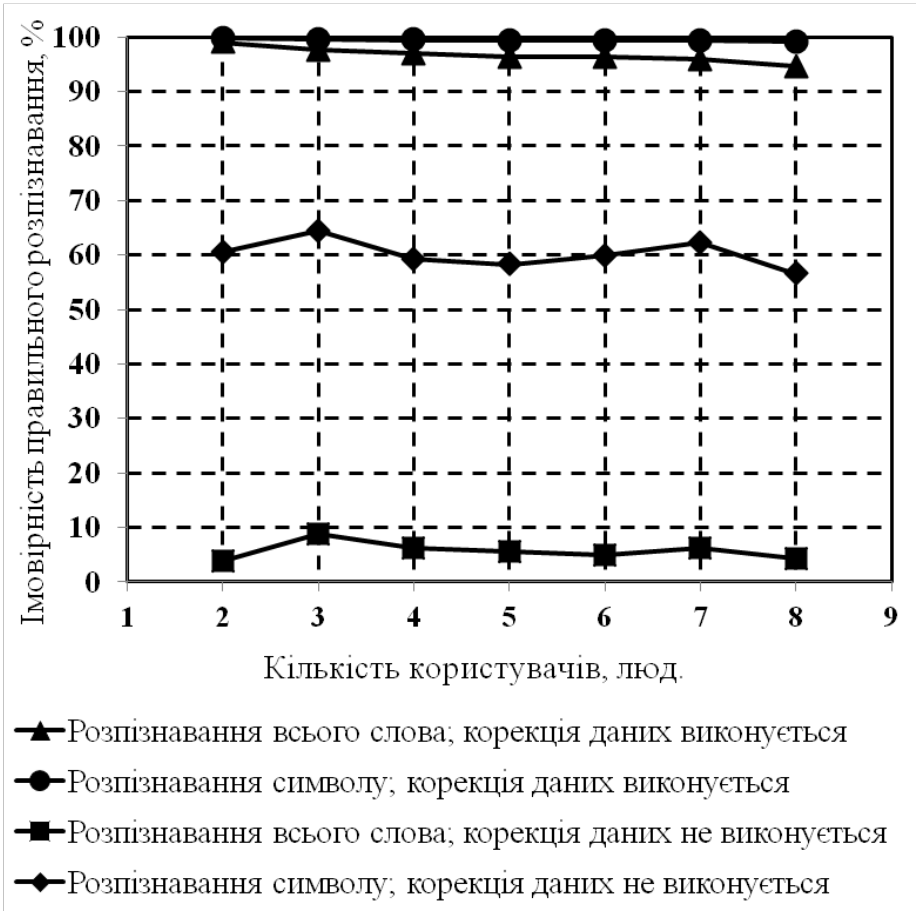


Рисунок 6.2.7 – Імовірність правильного розпізнавання користувачів інформаційних систем за їх рукописним почерком

6.3. Програмний застосунок методу ідентифікації функціонального профілю захисту системи підтримки прийняття рішень при проведенні експертиз комплексних систем захисту інформації

Невід'ємною складовою застосування будь-якої комплексної системи захисту інформації (КСЗІ) є проведення її експертизи. Відповідно було розроблено програмний застосунок методу ідентифікації функціонального профілю захисту (МІФПЗ) системи підтримки прийняття рішень при проведенні експертиз КСЗІ.

Вимоги та принципи побудови системи підтримки прийняття рішень при проведенні експертизи КСЗІ

Функціонал системи підтримки прийняття рішень (СППР) повинен задовольняти вимогам Закону України "Об інформації" та Закону України Про захист інформації в інформаційно-телекомунікаційних системах".

Програмний застосунок повинен мати функціонал (або можливість удосконалення програми для досягнення функціоналу в подальшому) для можливості програмної реалізації усіх модулів програми підтримки прийняття рішення при проведенні державної експертизи КСЗІ [27-35].

Функції СППР

Модуль виділення смислових змінних (МВСЗ). Модуль повинен забезпечити виділення смислових констант з вхідних документів шляхом формування сукупності визначених констант у базу знань та внести ці константи у шаблони вихідних документів за визначеним алгоритмом.

Підсистема модуля МВСЗ повинна забезпечити виконання наступних функцій:

- виділення смислових констант з вхідних документів;
- формування бази знань смислових констант.

Модуль МІФПЗ. Модуль повинен забезпечити відповідність ФПЗ трьом критеріям нормативного документу НД ТЗІ 2.5.004-99.

Підсистема модуля повинна забезпечити виконання наступних функцій:

— функціональний профіль захисту (ФПЗ) зобов'язаний включати в себе контроль цілісності КСЗІ;

— пов'язаність функціональних послуг безпеки (ФПБ) одна з одною згідно з НД ТЗІ 2.5.004-99;

— якщо послуга має усі 4-ри рівня, то в функціональному профілі захисту може бути тільки одна.

Модуль взаємодії з експертом (МВЕ). Модуль повинен забезпечити формальну відповідність ФПЗ формату опису ФПЗ, а також дати експерту, в інтерактивному режимі, можливість аналізу ФПБ згідно з нормативним документом НД ТЗІ 2.5.004-99.

Підсистема модуля повинна забезпечити виконання наступних функцій:

— перевірку опису ФПЗ;

— забезпечувати експерту можливість отримувати розширену інформацію про послугу в інтерактивному режимі при подіях типу mouse focus.

Програмна реалізація повинна мати графічний інтерфейс інтуїтивно зрозумілий для користувачів. Так як більшість користувачів працює в ОС Windows різних поколінь, то інтерфейс програми повинен бути Windows-орієнтованим та відповідати офіційним рекомендаціям корпорації Майкрософт для розробників і дизайнерів графічних інтерфейсів.

Програмне забезпечення повинне:

— бути стійким до хибних дій користувача (помилки у діях персоналу не повинні приводити до збоїв (відмов) у роботі програмного забезпечення);

— забезпечувати гарантований контроль вхідної та вихідної інформації;

— забезпечувати час відновлення після відмови (збоїв) визначений ДСТУ 50136 частина 1.4.

Вимоги до лінгвістичного забезпечення графічного інтерфейсу

Для розробки і розвитку програмних засобів мають застосовуватись мови програмування високого рівня.

Для взаємодії користувача з технічними засобами повинен використовуватися стандартний графічний інтерфейс, який дозволяє використовувати програмне забезпечення з максимальною ефективністю. Елементи графічного інтерфейсу повинні відображати текст українською мовою. Взаємодія повинна бути орієнтована на використання 101-клавішної клавіатури та маніпулятора типу "миша". Елементи взаємодії користувачів з компонентами системи мають базуватись на стандартах для організації графічного інтерфейсу користувача в сучасних програмних засобах.

Вимоги до стандартизації та уніфікації

Програмне забезпечення розробляється на основі розповсюджених операційних систем та інструментальних засобів програмування.

Вимоги до інформаційної безпеки

Процедура санкціонованого доступу до баз даних повинна бути розроблена, виходячи із вимог: запобігання несанкціонованого внесення змін або знищення баз даних; запобігання несанкціонованого використання інформації баз даних;

Технічні питання регламентованого доступу до інформації в базах даних можуть бути вирішені паролями, які оформлені через адміністратора СППР.

Архітектура СППР при проведенні експертиз КСЗІ

Відповідно до проведеного аналізу та вибору підходів для забезпечення необхідних функцій СППР при проведенні експертиз КСЗІ було запропоновано наступну архітектуру (див. рис. 6.3.1).

В процесі роботи СППР приймають участь наступні модулі:

- модуль МВСЗ;
- модуль МІФПЗ;
- модуль МВЕ;
- база знань.

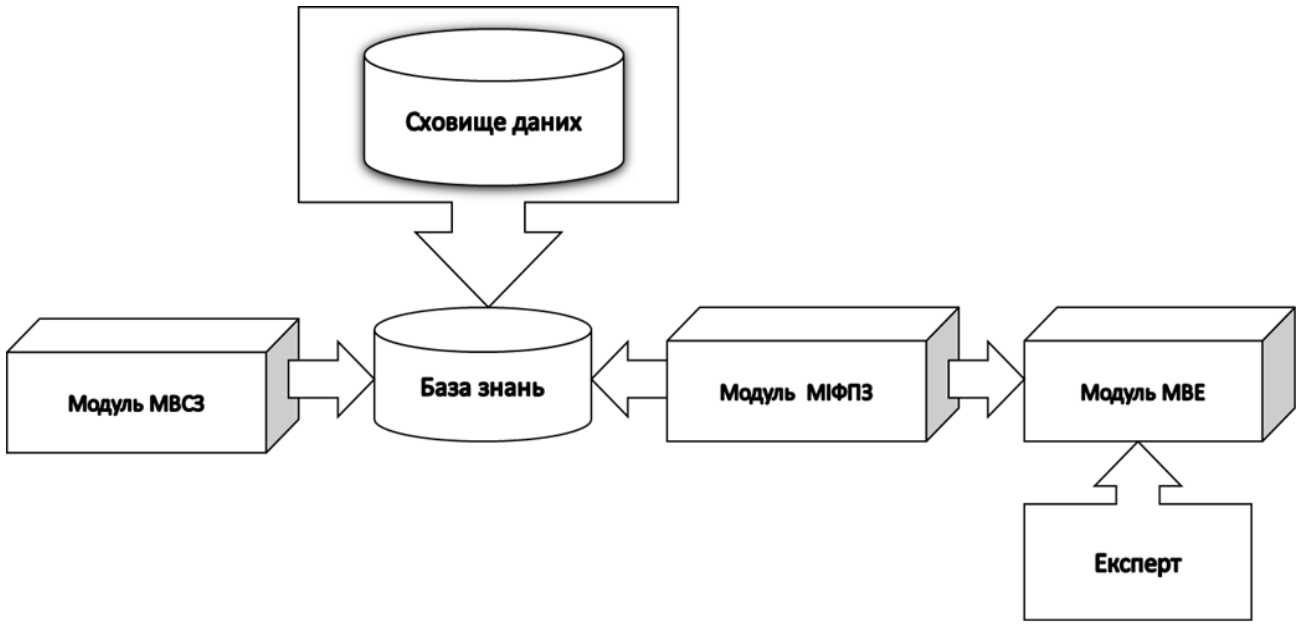


Рисунок 6.3.1– Компоненти СППР при проведенні експертиз КСЗІ

Узагальнений спрощений ланцюжок функціонування СППР:

— за допомогою МВЕ експерт взаємодіє з СППР. Модуль МВЕ призначений для наповнення (за участю експерта) шаблонів вихідних документів смисловими змінними, процесом генерування вихідних документів за допомогою відповідного інтерфейсу програми та аналізує множини критеріїв виокремленного з вхідних документів державних експертиз.

— модуль МВСЗ призначений для виокремлення смислових змінних з вхідних документів шляхом інтерактивної взаємодії експерта з інтерфейсом СППР за допомогою низки інструкцій.

— модуль МІФПЗ за рахунок виділення множин критеріїв з вхідних документів реалізує процес ідентифікації ФПЗ.

— база знань накопичує смислові змінні з вхідних документів, має в своєму складі шаблони вихідних документів для їх наповнення смисловими змінними та множин критеріїв для кожного проекту.

Програмний застосунок МІФПЗ

Враховуючи вищезазначене, було розроблено програмний застосунок СППР при проведенні експертиз КСЗІ, який аналізує вхідні документи на предмет

наявності ФПЗ і його ідентифікації за формальними ознаками НД ТЗІ (див. рис. 6.3.2) [27-35].

Реалізація програмного застосунка ідентифікації функціонального профілю захисту призначена для допомоги експерту при визначенні ФПЗ в документі Microsoft Word, а також допомагає експерту при аналізі ФПЗ. Головною метою цього програмного застосунка є допомога експерту при створенні ФПЗ та контроль на відповідність умовам заданим в нормативному документі НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», а саме: визначення контролю цілісності; поглинання старшими ФПЗ молодших; перевірка взаємопов'язаності ФПБ.

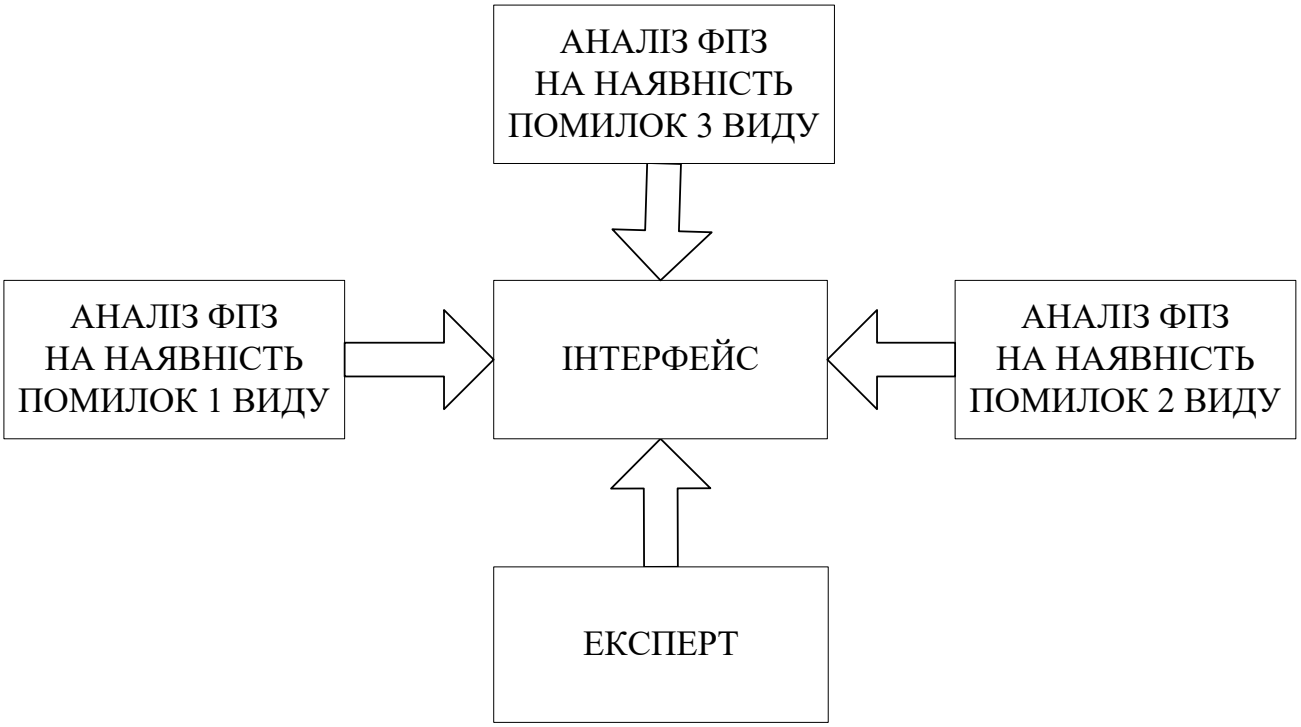


Рисунок 6.3.2 – Структурная схема программного застосунка СППР при проведенні експертиз КСЗІ

Програмний застосунок написано на мові програмування C# в середовищі розробки VisualStudio 2005. При написані програмного коду використовувалась технологія MSOffice'sCOMInterop, а саме бібліотека Microsoft.Office.Interop.Word та базові бібліотеки мови програмування C#.

Інтерфейс програмного застосунка представляє собою віконний додаток, яке реалізоване у вигляді GUI-програми, в якому є такі елементи управління: віконне поле типу «Listbox» пошуку функціонального профілю захисту; кнопок: «Знайти», «Зупинити», «Очистити»; права частина екрану має віконне поле типу «ListView», в якому відображується номер абзацу, де був знайдений профіль безпеки; три кнопки пошуку відповідності ФПЗ умовам нормативного документу НД ТЗІ 2.5-004-99; два віконних поля типу «TextBox» в одному з яких відображується загальна кількість абзаців документу, а в іншому полі поточний абзац при обробці документа; віконне поле типу «statusStrip», яке має три положення: «Очікую», «Пошук розпочато», «Пошук закінчено»; два віконних поля типу «CheckedBox» в одному з яких є можилвість зняти або обрати пошук ФПЗ, а в іншому полі є можливість переходу до заданої частини тексту пошуку ФПЗ; віконне поле типу «menuStrip», де розміщені дві вкладки: «Файл», «Допомога».

Аналіз ФПЗ за формальним ознаками можуть бути помилки 3 видів: 1 виду – відсутність ФПБ НЦ рівня визначеного експертом; 2 виду – перевірка на поглинання старшими ФПБ молодших; 3 виду – перевірка взаємопов’язаності ФПБ.

У випадку виявлення помилок в ФПЗ, інтерфейсом програмного застосунка експерту дається можливість виправити помилки та зберегти результат.

6.4. Програмне забезпечення грід-сервісу STRAGS віддаленого синтезу конфігурацій для реконфігуровних засобів захисту інформації

Вимоги та принципи побудови грід-сервісу STRAGS

При проектуванні грід-сервісу віддаленого синтезу конфігурацій для реконфігуровних засобів захисту інформації Security Tasks Reconfigurable Accelerators Grid-Service (STRAGS) було проведено аналіз програмного процесу локального синтезу конфігурацій та сформовано вимоги, яким має задовольняти

грід-сервіс [36-44]:

— на віддаленому грід-вузлі необхідно забезпечити наявність спеціалізованого програмного забезпечення для синтезу конфігурацій ПЛІС (в тому числі ліцензійного);

— забезпечити передачу вхідних даних (файлів опису апаратних компонент (VHDL-файлів) та файлів проекту) уніфікованим чином;

— можливість моніторингу поточного кроку синтезу проєкту для виявлення помилок на ранніх стадіях;

— прозоре для користувача керування процесом синтезу конфігурацій, а саме: запуск процесу синтезу в програмному забезпеченні шляхом відкриття файлу проекту.

Для забезпечення наявності спеціалізованого програмного забезпечення для синтезу обчислювальної структури для ПЛІС на обчислювальних елементах класичні підходи, а саме – встановлення під час роботи задачі та попередня інсталяція адміністратором цільового ресурсу мають ряд проблем та недоліків:

— розмір інсталяції програмного забезпечення – близько 10 Гб, тому його передача разом з файлами грід-завдання кожного разу не є доцільною;

— програмне забезпечення вимагає наявності ряду системних бібліотек (в т.ч. 32-бітних), які в загальному випадку відсутні на обчислювальних вузлах;

— навіть у випадку попередньої інсталяції адміністратором цільового ресурсу для кожного ресурсу існуватиме необхідність створення власних ресурсо-специфічних сценаріїв для забезпечення життєвого циклу задачі синтезу обчислювальної структури для ПЛІС та їх подальшого оновлення, що суттєво обмежує гнучкість використання грід-ресурсів

— у випадку ліцензійного програмного забезпечення немає можливості його встановлення на всі обчислювальні вузли всіх кластерів грід-сегменту;

— виходячи з вищезазначених міркувань для вирішення задачі забезпечення доступності програмного забезпечення було обрано новітню технологію, що була

створена в УНГ, яка забезпечує запуск віртуальної машини як грід-задачі за допомогою системи Rainbow (“ARC in the Cloud”) [44].

За використання такого підходу інсталяція всіх необхідних програмних залежностей та процеси створення та оновлення сценаріїв для забезпечення життєвого циклу задачі синтезу обчислювальної структури для ПЛІС зводяться до створення єдиного образу віртуальної машини, та його запуску на будь-якому обчислювальному кластері, незалежно від програмної конфігурації цільового обчислювального вузла.

Для уніфікації механізму передачі вхідних даних, що у загальному випадку представляють собою різні множини файлів та параметрів синтезу, з різними іменами файлів, тощо запропоновано використовувати архів з файлами проекту як атомарний об’єкт для проведення подальшого моделювання.

Такий підхід, з точки зору кінцевого користувача, дозволяє йому підготувати будь-який проект в графічному інтерфейсі програми синтезу обчислювальної структури для ПЛІС, після чого додати в архів всю директорію проекту та надіслати архів до грід-сервісу, який виконає синтез обчислювальної структури для ПЛІС (що вимагає суттєвого процесорного часу) в гріді та поверне готовий результат.

Для забезпечення моніторингу процесу синтезу на віддаленому грід-вузлі, з відображенням поточного кроку роботу, тощо, необхідно забезпечити постійний мережевий зв’язок між грід-сервісом та задачею. В класичному випадку, грід забезпечує лише доступ до потоків стандартного виводу та помилок завдання та не дозволяє здійснювати моніторинг процесів.

Враховуючи застосування віртуальних машин, було запропоновано підхід, що з використанням спеціалізованих сценаріїв всередині віртуальної машини, здійснює моніторинг процесу моделювання та передає дані безпосередньо на грід-сервіс. Повний контроль над програмним оточенням як грід-сервісу так і віртуальної машини дозволяє прозоро оновлювати та забезпечувати взаємодію цих компонентів незалежно від обраного обчислювального вузла в грід.

Архітектура грід-сервісу

Відповідно до проведеного аналізу та вибору підходів для забезпечення необхідних функцій віддаленого синтезу конфігурацій ПЛІС було запропоновано наступну архітектуру грід-сервісу (див. рис. 6.4.1).

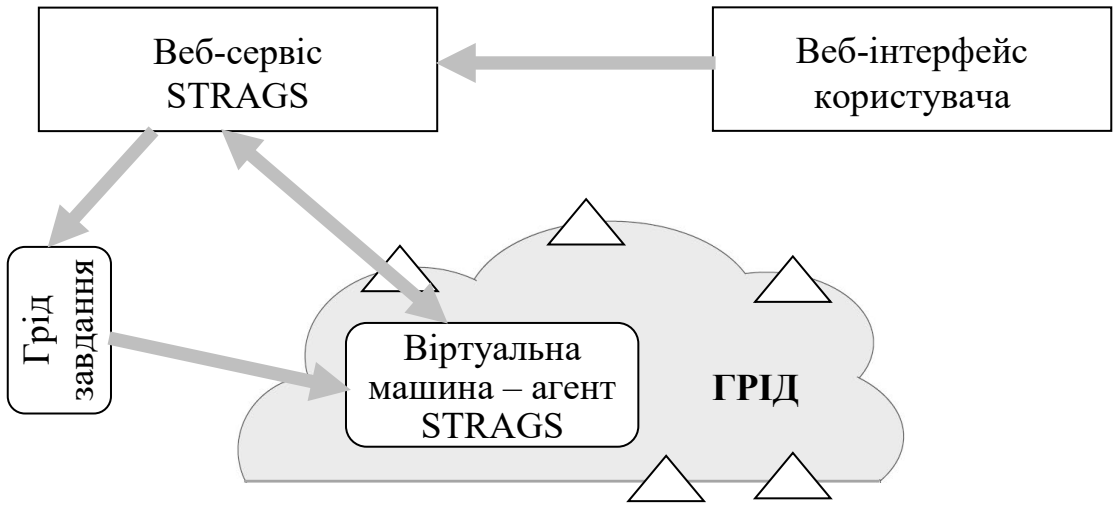


Рисунок 6.4.1 – Компоненти грід-сервісу STRAGS

В процесі віддаленого синтезу конфігурацій ПЛІС приймають участь наступні компоненти грід-сервісу:

- веб-сервіс STRAGS;
- віртуальна машина (запущена як грід-завдання) – агент STRAGS;
- веб-інтерфейс користувача.

Узагальнений спрощений технологічний ланцюжок функціонування системи наступний:

За допомогою веб-інтерфейсу, користувач (авторизуючись за допомогою персонального сертифікату) надсилає архів проекту до сервісу STRAGS.

Архів та метадані щодо проекту зберігаються в базі даних сервісу STRAGS.

Сервіс STRAGS від імені службового грід-сертифікату надсилає до грід-інфраструктури завдання.

Грід-завдання, використовуючи набір програмних компонентів Rainbow, запускає віртуальну машину – агент STRAGS.

Агент STRAGS повідомляє про свою готовність приймати завдання сервісу STRAGS.

Агент STRAGS отримує архів з проектом та виконує запуск процесу моделювання конфігурації ПЛІС.

На протязі процесу моделювання агент STRAGS здійснює моніторинг стану завдання та надсилає результати моніторингу сервісу STRAGS.

Результати моніторингу зберігаються в базі даних сервісу STRAGS та можуть бути переглянуті за допомогою веб-інтерфейсу користувача.

По завершенні моделювання, бінарний файл конфігурації ПЛІС та журнали виконання завдання передаються агентом на сервіс STRAGS.

Агент STRAGS повертається до стану готовності і протягом часу роботи грід-завдання може прийняти інше завдання для моделювання.

Користувач завантажує результати роботи та журнали за допомогою веб-інтерфейсу.

Веб-сервіс STRAGS є точкою взаємодіє користувачів сервісу з грід-інфраструктурою і відповідно складається з ряду компонентів, які забезпечують роботу з грід-вузлами, обмін завданнями з користувачами а STRAGS-агентами (див. рис. 6.4.2).

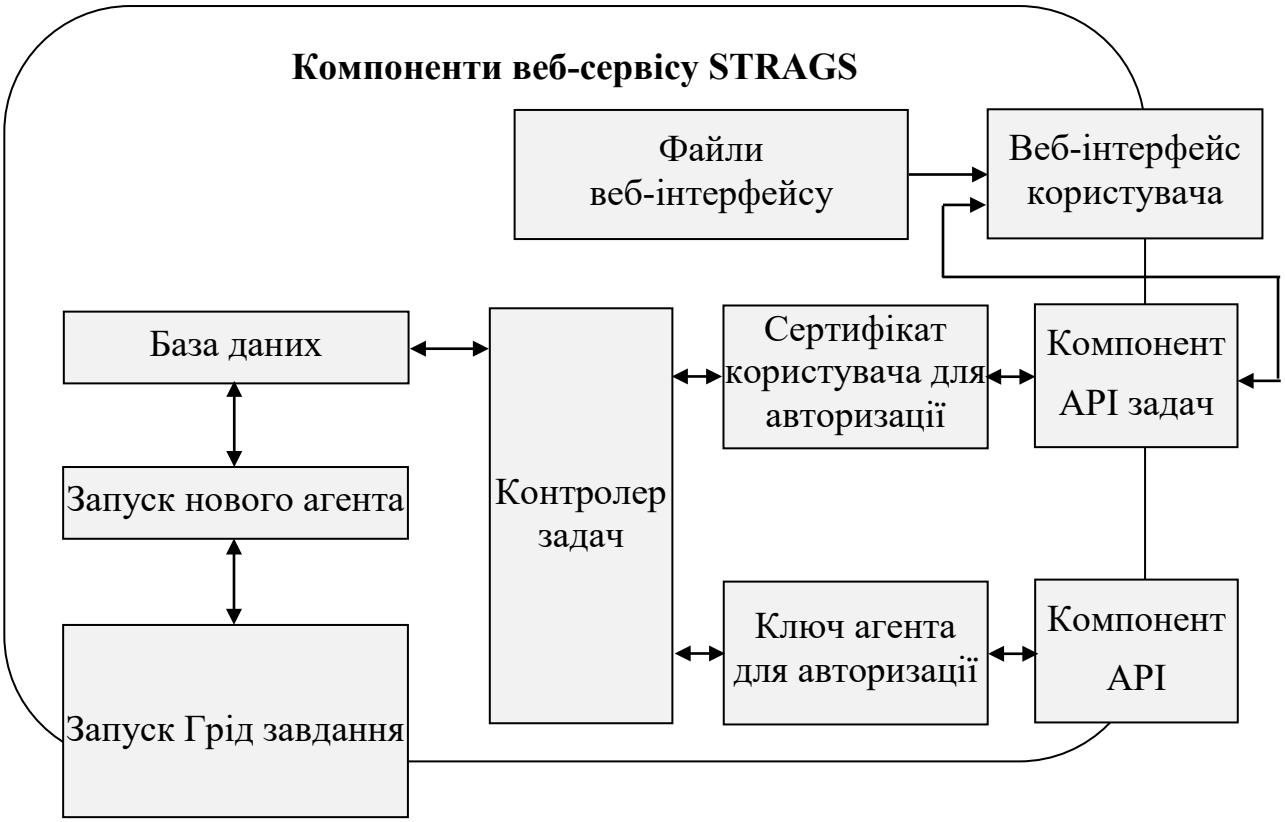


Рисунок 6.4.2 – Компоненти веб-сервісу

База даних (Database) зберігає всю інформацію як про запущені агенти так і про наявні та виконані завдання та їх власників.

Запуск нових агентів відбувається з використанням інформації з бази даних, а саме – поточна кількість завдань, що очкують на виконання, загальна кількість запущених агентів та кількість вільних агентів. При збільшенні кількості завдань запускаються нові агенти, при зменшенні – система забезпечує роботу мінімальної кількості агентів, що в поточній програмній реалізації встановлено у кількості трьох примірників.

Процес запуску нового агенту (Agents Submission) складається з наступних етапів:

— генерація нового ключа для авторизації агенту та збереження його в базі даних;

— генерація проксі-сертифікату (використовується сертифікат вузла strags.matmoden.kiev.ua на базі ВО "MatModEn");

— створення файлу конфігурації клієнтів Nordugrid ARC з зазначенням індексів інформаційної системи УНГ;

— створення файлу опису завдання в якому: а) вказується шлях до образу диску віртуальної машини-агенту, б) запитується використання Rainbow, в) передається ключ авторизації агенту, г) визначаються параметри запуску віртуальної машини;

— надсилання завдання до грід-інфраструктури.

Додавання нових завдань, а також моніторинг та керування існуючими завданнями здійснюється через API задач (Jobs API), який реалізує всі зазначені операції:

— додавання нової задачі;

— перегляд стану та етапу виконання запущених задач;

— перегляд обрахованих задач;

— отримання бінарного файлу конфігурації ПЛІС;

— отримання журналів процесу моделювання конфігурації ПЛІС;

— перезапуск завдання;

— видалення завдання і файлів з сервісу.

Всі запити проходять через ланку авторизації з використанням персонального сертифікату користувача (TLS AuthZ) і не можуть бути виконані в обхід механізму авторизації.

Після успішної авторизації запити передаються на контролер задач (Jobs Controller), що здійснює їх обробку: збереження та модифікація інформації в базі даних та на диску, повернення результату обробки в API.

Веб-інтерфейс користувача (Web UI) в рамках архітектури грід-сервісу STRAGS є незалежним компонентом, що взаємодіє з веб-сервісом виключно через API. Проте файли самого веб-інтерфейсу (Web Content) зберігаються на сервері та передаються клієнту за протоколом HTTP. Отримавши файли, веб-браузер інтерпретує код веб-клієнту і здійснює запити в API.

Для взаємодії з агентами реалізовано окремий API (Agent API), який забезпечує:

— відслідковування стану агенту;

— передача проекту на обрахунок;

— моніторинг процесу обрахунку;

— отримання результатів.

Взаємодія через Agent API завжди проходить ланку авторизації по ключу агента, який генерується та передається на етапі запуску грід-завдання (Agent KEY AuthZ). Конфіденційність та цілісність передачі даних між агентом та сервісом забезпечується використанням TLS (використовується сертифікат сервісу STRAGS) а ідентифікація та авторизація виконується за допомогою спільного ключа кожного агенту (на відміну від ідентифікації та авторизації за допомогою персонального сертифікату користувача).

Після успішної авторизації запити передаються на контролер задач (Jobs Controller), що здійснює їх обробку: збереження та модифікація інформації в базі даних та на диску, повернення результату обробки в API.

Робота віртуальної машини – агенту STRAGS забезпечується наступними програмними компонентами (див. рис. 6.4.3):

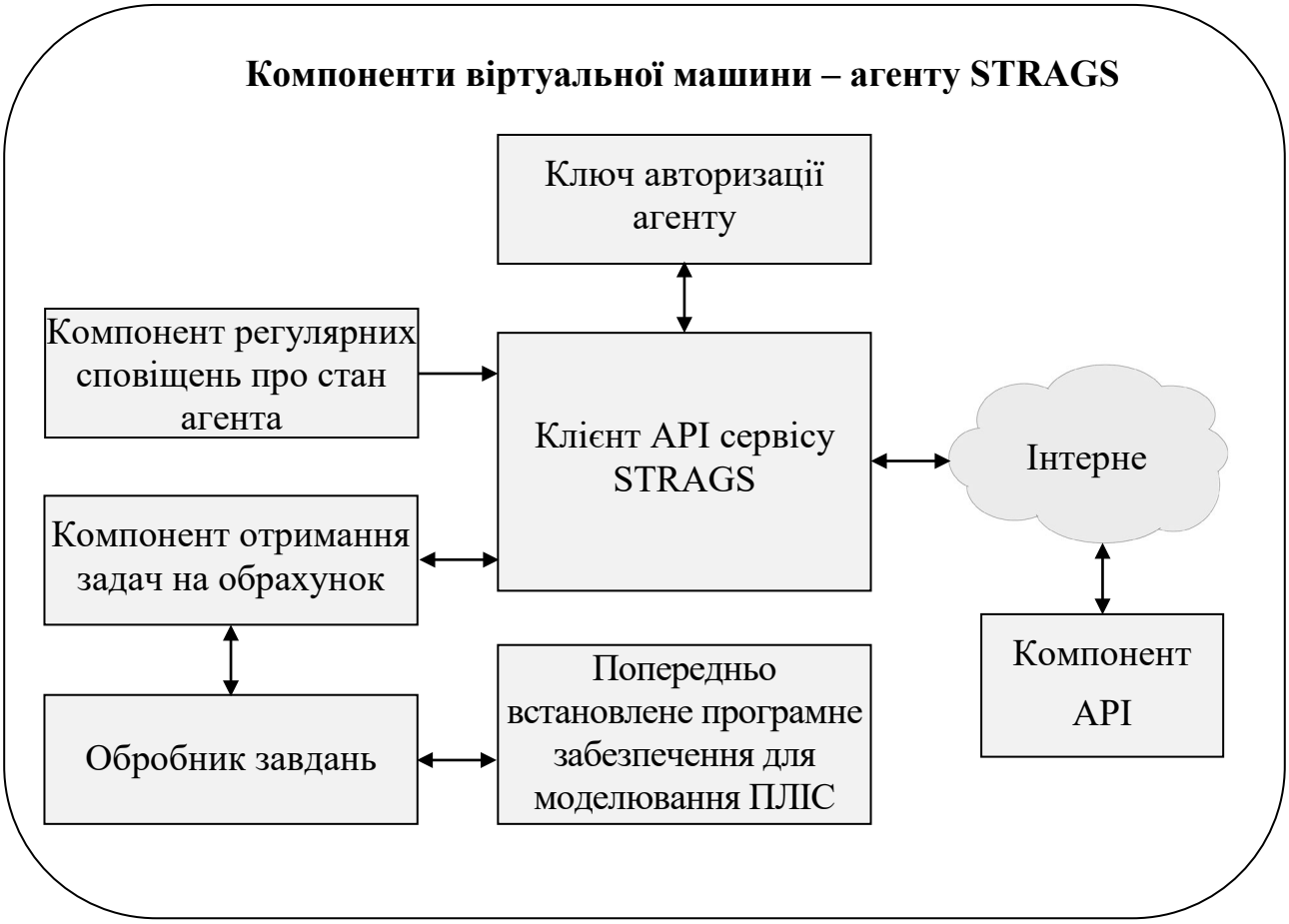


Рисунок 6.4.3 – Компоненти віртуальної машини – агенту STRAGS

1. Наперед встановлене та налаштоване програмне забезпечення з компіляції проєкту та синтезу конфігурації для ПЛІС.

Обробник завдань (Jobs Processor) – сценарій забезпечення життєвого циклу розрахунку, який: а) визначає тип архіву, б) виконує розархівацію, в) визначає ім’я файлу проекту, г) визначає параметри виконання проекту, д) виконує поетапне виконання процесу синтезу конфігурації, є) здійснює контроль за безпомилковим виконанням кожного етапу.

Ключ авторизації агенту (Agent KEY) – передається віртуальній машині на етапі запуску виходячи з опису грід-завдання.

Клієнт API сервісу STRAGS (Agent API Client) – виконує загальні функції для взаємодії з API сервісу STRAGS, включаючи обробку авторизації по ключу агента.

Agent Heartbeat – регулярні сповіщення про стан агента, що дозволяють сервісу отримувати актуальну інформацію про кількість доступних та завантажених задачами агентів. Грід-інфраструктура є розподіленою і вихід з ладу певного обчислювального кластеру не повинен впливати на роботу сервісу. Надсилаючи періодичні повідомлення про свій стан агент підтверджує свою працездатність. У випадку виходу з ладу вузла де працював агент, сервіс не отримує повідомлення про стан і через певний час запускає новий агент на заміну.

Оновлення програмних компонентів агенту STRAGS виконується на етапі виконання Agent Heartbeat – поточна версія компонентів передається на сервіс протягом сповіщення про стан, і у випадку якщо вона менше необхідної для роботи сервісу – агент отримує команду щодо необхідності оновлення. Це забезпечує цілісність роботи системи без необхідності перезапуску існуючих агентів через оновлення.

Отримання задач на обрахунок (Jobs Retrieval) – звертається до сервісу та запитує нові завдання, скачує архів з проектом та передає його на виконання обробнику завдань. Здійснює моніторинг процесу виконання та сповіщає про зміну стану завдання (етапу виконання) на сервер.

Програмна реалізація грід-сервісу

Веб-сервіс. Компоненти веб-сервісу виконані мовою програмування PHP, використовують веб-сервер Apache та базу даних MySQL. (Структура бази даних сервісу STRAGS мовою SQL наведена нижче) Apache налаштований на авторизацію по персональним сертифікатам користувачів, результати якої обробляються в PHP.

Для запуску завдань-агентів використовуються SHELL-сценарії, що для взаємодії з грід-інфраструктурою викликають бінарні клієнти Nordugrid ARC.

API реалізовано за допомогою REST-підходу з використанням семантики JSON.

Веб-інтерфейс користувача. Веб інтерфейс створено за допомогою використання стилів Twitter Bootstrap та бібліотек jQuery для здійснення AJAX запитів в JSON API веб-серверу.

Агент STRAGS. Створена віртуальна машина працює під керування ОС Scientific Linux 6.7 на яку встановлено фірмовий програмний пакет САПР Xilinx WebPACK ISE ver.10.1 та всі необхідні програмні компоненти для його роботи.

Реалізацію компонентів агенту виконано мовою Python, включаючи клієнт JSON API та всі операції взаємодії з сервером. Обробник завдань виконано як SHELL-сценарій що викликає команди наперед встановленого програмного забезпечення для моделювання конфігурації ПЛІС.

6.5. Висновки до шостого розділу

В шостому розділі показані розроблені програмні застосунки безпеки систем розмежування доступу та інші розробки. Їх експериментальні дослідження, а також їх впровадження та успішне практичне використання, підтвердили достовірність теоретичних положень і висновків дисертаційної роботи.

Список використаних джерел до шостого розділу

1. А. М. Давиденко, О. А. Суліма, О. А. Давиденко, «Використання дворівневої моделі доступу до даних для вирішення прикладної задачі з проведення об'єкту по території з обмеженим доступом», *Моделювання та інформаційні технології. Зб. наук. праць*, Вип. 80, С.95-100, 2017.

2. 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.

3. Суліма О. А. Аналіз процесів надання повноважень в інформаційно-телекомунікаційних системах / О. А. Суліма. — Харків : Технологічний центр, 2016.

4. Суліма О. А. Особливості використання засобів визначення повноважень в державних інформаційних системах / О. А. Суліма. — К. : ІПМЕ ім. Г.Є. Пухова НАНУ, 2016.

5. Редько В. Г. Эволюция, нейронные сети, интеллект : модели и концепции эволюционной кибернетики / В. Г. Редько. — М. : Ленанд, 2015. — 220 с.

6. Гладков Л. А. Генетические алгоритмы / Л. А. Гладков, В. В. Курейчик, В. М. Курейчик. — М. : ФИЗМАТЛИТ, 2006. — 320 с.

7. Акимов О. Е. Дискретная математика: логика, группы, графы, фракталы / О. Е. Акимов. — М. : АКИМОВА, 2005. — 656 с.

8. А. Давиденко, О. Суліма, «Використання формальних засобів опису процесів надання повноважень», Захист інформації, Том 18, №2, С.143-149, 2016.

9. 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.

10. А. М. Давиденко, О. А. Суліма, «Структурні підходи до методів оцінки рівня безпеки інформаційних систем», *Моделювання та інформаційні технології. Зб. наук. праць*, Вип. 83, С.11-21, 2018.

11. А. М. Давиденко, О. А. Суліма, «Аналіз функціональних можливостей окремих компонент засобів захисту інформаційних систем», *Моделювання та інформаційні технології. Зб. наук. праць*, Вип. 84, С.103-111, 2018.

12. A. Davydenko, O. Sulima, O. Vysotska, S. Hilgurt, «A study case of the implementation of a multi-layered access system to manage the procedures for using confidential information without violating the security policy», *Захист інформації і безпека інформаційних систем: VII Міжнародна науково-технічна конференція*, Львів, 2019, С.27-28.

13. А.М. Давиденко, О.А. Суліма, О.О. Політучий, «Реалізація процесів адаптації при вирішенні завдань захисту систем доступу до інформаційних об'єктів енергетики», *Кібербезпека енергетики*: *науково-практична конференція*, Одеса, 2019, С.16-20.

14. Lee, C.Y., «An Algorithm for Path Connections and Its Applications», IRE Transactions on Electronic Computers, vol. EC-10, number 2, pp. 364—365, 1961

15. Обход препятствий: волновой алгоритм (Алгоритм Ли), [Електронний ресурс], Режим доступу: https://suvitruf.ru/2012/05/13/1176/volnovoj-algoritm-algoritm-li/

16. Алгоритм Ли, [Електронний ресурс], Режим доступу: https://amp.ru.googl-info.com/1543734/1/algoritm-li.html

17. O.Vysotska, A.Davydenko, «Keystroke Pattern Authentication of Computer Systems Users as One of the Steps of Multifactor Authentication», *Advances in Computer Science for Engineering and Education II. Advances in Intelligent Systems and Computing*, vol. 938, pp. 356-368, 2019.

18. A. Davydenko, O. Vysotska, T. Shmelova, «Methods of Primary Processing Handwriting Samples at User Authentication Using a Probabilistic Neural Network*», 1st International Conference on Cyber Hygiene and Conflict Management in Global Information Networks (CyberConf 2019)*, Kyiv, Ukraine, 2019., pp. 723-735.

19. Е.Высоцкая, А.Давиденко, «Исследование эффективности применения вероятностных нейронных сетей для решения задачи аутентификации пользователя компьютерных систем», *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Наук.-техн. зб.*, Вип. 9, С. 103-110, 2004.

20. Е.А.Высоцкая, А.Н.Давиденко, «Анализ технологии предварительной обработки данных при аутентификации пользователей компьютерных систем по

клавиатурному и рукописному почеркам», *Моделювання та інформаційні технології. Зб. наук. праць*, Вип. 55, С. 34-41, 2010.

21. А.М.Давиденко, О.О.Висоцька, «Визначення функції моніторингу стану санкціонованих користувачів комп'ютерних систем за допомогою аналізу їх клавіатурного почерку», *Комп'ютерні системи та мережні технології (CSNT-2019): XII Міжнародна науково-практична конф.*, Київ, 2019, С.41-42.

22. А.М.Давиденко, О.О.Висоцька, «Моніторинг функціонального стану представників критичних професій, за допомогою аналізу їх клавіатурного почерку», *Актуальні проблеми управління інформаційною безпекою держави: X Всеукраїнська науково-практична конференція*, Київ, 2019, С.201-203.

23. O.Vysotska, A.Davydenko, «Authentication of information systems users, based on the analysis of their handwriting», *Scientific and Practical Cyber Security Journal (SPCSJ)*, vol.2, no.4, pp. 51-63, 2018.

24. О.Корченко, А.Давиденко, О.Висоцька, «Метод автентифікації користувачів інформаційних систем за їх рукописним почерком з багатокроковою корекцією первинних даних», *Захист інформації*, Том 21, №1, С. 40-51, 2019.

25. O.Vysotska, A.Davydenko, «The usage of handwriting recognition systems of information systems users for their authentication», *La science et la technologie à l'ère de la société de l'information: conférence scientifique et pratique internationale*, Bordeaux, France, 2019, vol.9, pp.48-51.

26. О.Висоцька, А.Давиденко, В.Щербина, «Формалізація процедури аналізу рукописного почерку людини для організації розмежування доступу до інформаційних систем», *ITSec: Безпека інформаційних технологій: IX Міжнародна науково-технічна конф.*, Київ (Україна), Шарм-ель-Шейх (Египет), 2019, С.22-23.

27. О. Корченко, А. Давиденко, М. Шабан, «Декомпозиційна модель представлення смислових констант та змінних для реалізації експертиз у сфері ТЗІ», *Захист інформації*, Том 21, № 2, С. 88-96, 2019.

28. О. Корченко, А. Давиденко, М. Шабан, «Модель параметрів для ідентифікації функціонального профілю захисту в комп'ютерних системах», *Безпека інформації*, Том 25, № 2, С.122-126, 2019.

29. О. Корченко, А. Давиденко, М. Шабан, І. Іванченко, «Метод ідентифікації функціонального профілю захисту», *Захист інформації*, Том 21, № 4, С.252-258, 2019.

30. А. Корченко, А. Давиденко, М. Шабан, С. Казмірчук, «Структурна модель СППР при проведенні державних експертиз КСЗІ», *Безпека інформації*, Том 26, № 1, С.14-27, 2020.

31. А. Н. Давиденко, М. Р. Шабан, «Разработка методики проведения экспертизы комплексных систем защиты информации», *Моделювання та інформаційні технології. Зб. наук. праць*, Вип. 73, С.114-221, 2014.

32. М.Р. Шабан, М.П. Карпінський, О.Г. Корченко, А.М. Давиденко, «Розробка методу ідентифікації функціональних профілей захисту», *Актуальні питання забезпечення кібербезпеки та захисту інформації: VI Міжнародна науково-практична конференція*, Київ, 2020, С.113-116.

33. О. Корченко, А. Давиденко, М. Шабан, «Формування критеріїв для функціонального профілю захисту», *ITSec: Безпека інформаційних технологій: X Міжнародна науково-технічна конференція*, Київ (Україна), Шарм-ель-Шейх (Египет), 2020, С.35-36.

34. А.М. Давиденко, М.Р. Шабан, В.П. Щербина, «Структурна модель СППР для проведення експертиз КСЗІ», *Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS'2020): XII Всеукраїнська науково-практична конференція*, Коблево, 2020, С.19-20.

35. А.М. Давиденко, С.Я. Гільгурт, М.Р. Шабан, «Апаратно-програмний комплекс підтримки прийняття рішень при проведенні державних експертиз комплексних систем захисту інформації», *Патент UA 139730 U; G06F17/27*. Патент опубліковано 10.01.2020, бюл. № 1.

36. A. Salnikov, A. Davydenko, «Web-service for FPGA synthesis using ARC-powered grid infrastructure», *Annual NorduGrid Conference 2017*, Tromsø, Norway, 2017.

37. В. Евдокимов, А. Давиденко, С. Гильгурт, «Централизованный синтез реконфигурируемых аппаратных средств информационной безопасности на высокопроизводительных платформах», *Захист інформації*, Том. 20, № 4, С.247-258, 2018.

38. В. Ф. Евдокимов, А. Н. Давиденко, С. Я. Гильгурт, «Организация централизованной генерации файлов конфигураций для аппаратных ускорителей задач информационной безопасности», *Моделювання та інформаційні технології. Зб. наук. праць*, Вип. 81, С.3-11, 2017.

39. А.Н. Давыденко, С.Я. Гильгурт, «Применение грид-сети для синтеза промышленных систем защиты информации на базе ПЛИС», *Цифровые технологии в промышленности: республиканской научно-практической конференции*, Актау, Казахстан, 2019. С.15-20.

40. Є.А. Слюсар, О.О. Судаков, Ю.В. Бойко, «Методики забезпечення високої доступності та балансування навантаження служб рівня кооперації в українській національній грід-інфраструктурі», *Моделювання та інформаційні технології: Зб. наук. пр.*, № 64, С. 28-35, 2012.

41. Є.А. Слюсар, «Комплексна система тестування взаємодії ресурсів у національній грід-інфраструктурі», *Проблеми програмування*, № 2-3, С. 111-118, 2012.

42. Е.А. Слюсар, «Автоматизированная служба репликации файлов для организации высокой доступности данных в грид-инфраструктуре», *УСиМ: Управляющие системы и машины*, № 4, С. 63-74, 2012.

43. А.А. Сальников, «Масштабована грід-служба керування участю в віртуальних організаціях», *Управляющие системы и машины*, № 4, С. 51-62, 2012.

44. А.А. Сальников, В.В. Вишневский, А.Ф. Борецкий, «Платформа как сервис» в грид для интерактивного анализа медицинских данных», *Математичні машини і системи*, Вип. 1, С. 53-64, 2015.

ВИСНОВКИ

В дисертаційній роботі, на основі проведених досліджень, вирішена нова важлива науково-технічна проблема, яка полягає у створенні методів та моделей побудови та організації процесу функціонування засобів захисту для систем доступу до розподілених інформаційних систем, що вирішують протиріччя між паралельними методами обробки інформації та послідовної організацію захисту, завдяки чому засоби захисту здатні адаптуватися до алгоритмів доступу, що змінюються в процесі її функціонування. При цьому отримано наступні результати:

1.Проаналізовано сучасні методи та моделі розмежування доступу до ресурсів інформаційних систем. Встановлено, що однопотокові механізми розмежування доступу не можуть забезпечити високі вимоги для високопродуктивної обробки інформаційних ресурсів з обмеженим доступом, в той же час спостерігається постійне зростання продуктивності обчислювальних систем, тому запропоновано наділити підсистему захисту властивостями адаптації по відношенню до критеріїв, які визначаються параметрами стану безпеки системи та параметрами, що характеризують процеси обробки інформації у спеціалізованих розподілених інформаційних системах.

2.Удосконалено структурну модель нейрона, в яку інтегровано блок пам’яті та блок аналізу, які комутуються до блоку підсумовування вхідних параметрів та формують зворотний зв’язок з функціональними змінними нейрона. Зазначена модель дозволяє в межах окремого нейрона запам’ятовувати часовий тренд його вагових параметрів на визначеному часовому інтервалі, завдяки чому з’являється новий функціонал організації контролю даних в системах розмежування доступу.

3.Отримав подальший розвиток метод самоорганізації засобів розмежування доступу, в якому за рахунок застосування правила Хебба та відповідної модифікації адаптаційної залежності, для випадку формування вхідних сигналів які не містять постійної складової, сформовано співвідношення для побудови рекурентного алгоритму на базі односпрямованої нейронної мережі. Зазначений

метод дозволяє автоматизувати процеси модифікації елементів засобів захисту по відношенню до стану параметрів безпеки системи розмежування доступу.

4.Вперше розроблено структурну модель засобів інформаційного забезпечення системи розмежування доступу, в якій за рахунок сюр'єкції множин ідентифікаторів предметних областей користувачів та об'єктів доступу формуються бієкції та набір семантичних правил, які узагальнюють процес вирішення завдання побудови взаємозворотних перетворень. Зазначена модель дозволяє побудувати метод адаптації системи контролю доступу та сформувати відповідні критерії.

5.Вперше запропоновано метод адаптації системи розмежування доступу, на основі генерування зміни оцінки значень параметрів та регулювання їх кількості при збереженні логіки аналізу. Зазначений метод дозволяє побудувати систему розмежування доступу, яка набуває нового функціоналу автоматичного інкременту або декременту кількості механізмів захисту при відповідній варіабельності стану безпеки ресурсів інформаційних систем.

6.Удосконалено метод аналізу системи розмежування доступу, шляхом консолідації оцінки рівня захищеності індивідуальних елементів об'єкта доступу, множини загроз, множини зав'язків із зовнішнім оточенням, функціонального завантаження об'єкта доступу та параметру навантаження обчислювальних ресурсів. Зазначений метод дозволяє отримати комплексну оцінку стану безпеки системи розмежування доступу.

7.Вперше розроблено структурно-функціональну декомпозиційну модель системи розмежування доступу, в якій інтегровано блоки аналізу результатів реалізованого доступу, аналізу ситуації відмови в доступі, критеріїв адаптації засобів захисту відповідно до поточного стану безпеки кібердовкілля та керування засобами захисту системи розмежування доступу. Зазначена модель дозволяє реалізувати запропонований метод адаптації системи розмежування доступу до розподілених інформаційних ресурсів шляхом розробки та рекомбінації її окремих компонентів.

8.Розроблено грід-сервіс віддаленого синтезу конфігурацій для реконфігуровних засобів захисту інформації Security Tasks Reconfigurable Accelerators Grid-Service на базі гріду та хмарної інфраструктури Українського національного гріду, що підтверджується актом від 28.12.2019 р. по договору №213-19 від 29.03.2019р.

9.Розроблено апаратно-програмний комплекс підтримки прийняття рішень при проведенні державних експертиз комплексних систем захисту інформації, Патент UA 139730 U; G06F17/27. Патент опубліковано 10.01.2020, бюл. № 1.

10.Розроблено апаратно-програмний комплекс моніторингу та керування технологічним процесом зневоднення бішофіту, Патент UA 140326 U; G05B15/00, G05B19/00. Патент опубліковано 10.02.2020, Бюл. № 3.

Розроблені в роботі моделі та методи адаптації засобів захисту, використовувались при реалізації систем контролю доступу, окремих механізмів захисту та побудови моделей загроз та порушника, а також програм та методик випробувань при проведенні державних експертиз комплексних систем захисту за дорученням ДССЗЗІ СБУ України: Центру реєстрації віртуальних організацій української національної грід-інфраструктури Київського національного університету імені Тараса Шевченка, Українського академічного грід-вузла Інституту теоретичної фізики ім. М.М. Боголюбова Національної академії наук України, автоматизованої інформаційної системи Президії Національної академії наук України, автоматизованої системи класу «2» Ресурсного центру Інституту кібернетики Національної академії наук України, локальної обчислювальної мережі Управління справами Національної академії наук України, автоматизованої системи класу «2» для підготовки даних Департаменту військово-технічної політики, розвитку озброєння та військової техніки Міністерства оборони України, автоматизованої системи для обробки відкритої інформації Центрального науково-дослідного інституту озброєння та військової техніки Збройних Сил України, що підтверджується атестатами відповідності: №9435 від 13.12.2013 р., №9434 від 13.12.2013 р., №11800 від 29.12.2014 р., №14680 від 29.12.2016 р., №14757 від 27.01.2017 р., №17407 від 07.09.2018 р., №19159 від 08.05.2019 р.

Розроблені в дисертаційній роботі методи побудови засобів захисту на основі використання математичних моделей використовувались в науково-дослідних роботах, що проводились в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України за темами «Кріт», «МодА», «МодБ», «МодД», «Управление», «Модель» та виконувались у відповідності з замовленням Президії академії наук України, а також у роботах за цільовими комплексними програмами відповідно до договорів №200-12 від 30.03.2012р., №200-13 від 01.03.2013р., №205-15 від 06.04.2015р., №206-16 від 15.04.2016р., №210-18 від 16.04.2018р., №213-19 від 29.03.2019р., №213-20 від 15.05.2020р., що підтверджується звітами виконаних робіт: №0101U006700 від 31.12.2004р., №0105U001296 від 31.12.2008р., №0108U010588 від 31.12.2013р., №0114U002361 від 31.12.2018р., №0102U005589 від 29.12.2006, №0107U001945 від 31.12.2009р., №0112U004018 від 25.12.2012р., №0113U002457 від 25.12.2013р,. №0115U002876 від 31.12.2015, №0116U006907 від 31.12.2016р., №0118U001370 від 28.12.2018р., №0119U001812 від 28.12.2019р., №0119U001812 від 28.12.2020р.

Результати дисертації впроваджено у діяльність Інституту кібернетики імені В.М. Глушкова Національної академії наук України, ТОВ «Софтлайн ІТ», НДЦ «Нафтогазбурмаш», Департаменту військово-технічної політики, розвитку озброєння та військової техніки Міністерства оборони України, Центральному науково-дослідному інституту озброєння та військової техніки Збройних Сил України, а також використовувалась в навчальному процесі Київського національного університету імені Тараса Шевченка, Національного авіаційного університету для підготовки фахівців з кібербезпеки, що підтверджується актами впровадження: від 19.12.2017р., від 03.12.2018р., від 16.12.2019р., 30.12.2019р., від 05.11.2019р., від 02.08.2017р.

Експериментальні дослідження програмних застосунків безпеки систем розмежування доступу та інших розробок, а також їх впровадження і успішне практичне використання, підтвердили достовірність теоретичних положень і висновків дисертаційної роботи.

ДОДАТОК А. ДОКУМЕНТИ, ЩО ПІДТВЕРДЖУЮТЬ ВПРОВАДЖЕННЯ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЙНОЇ РОБОТИ

Акти впровадження

ЗАТВЕРДЖУЮ

Проректор з навчальної та виховної роботи Національного авіаційного університету

_____ Т. Іванцова

«02» 08 2017 р.

АКТ

впровадження у навчальний процес Національного авіаційного університету результатів дисертаційної роботи Давиденко Анатолія Миколайовича «Методи та моделі функціонування адаптивних засобів захисту доступу до інформаційних систем» на здобуття наукового ступеня доктора технічних наук.

Комісія у складі: голова –завідувач 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 Давиденко Анатолія Миколайовича «Методи та моделі функціонування адаптивних засобів захисту доступу до інформаційних систем» 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.	Розширення математичної моделі елементу нейронної мережі, що дозволило розширити його функціональні можливості, завдяки чому в рамках окремого нейрона стало можливим запам'ятовувати часовий тренд його вагових параметрів на визначеному часовому інтервалі.	Лекція	Ознайомлення студентів з застосуванням нейронних мереж для керування та оцінки параметрів систем захисту інформації.
2.	Методи використання семантичних параметрів для аналізу поточного стану системи захисту та виявлення змін міри захищеності ресурсів комп'ютерної мережі, яка надає послуги користувачам.	Лекція	Ознайомлення студентів з методами формального опису параметрів даних, що зберігаються в системі доступу до ресурсів інформаційних систем, що дозволило побудувати процедуру визначення моменту налаштування системи захисту.

Голова комісії,
завідувач кафедри безпеки інформаційних технологій О. Корченко

Члени комісії:

професор кафедри безпеки інформаційних технологій Є. Іванченко

доцент кафедри безпеки інформаційних технологій Т. Жмурко

ЗАТВЕРДЖУЮ

Учений секретар
доктор фіз.-мат. наук
_____ С. В. ЄРШОВ
«19» 12 2017 р.

АКТ

впровадження результатів дисертаційної роботи Давиденко Анатолія Миколайовича «Методи та моделі функціонування адаптивних засобів захисту доступу до інформаційних систем» на здобуття наукового ступеню доктора технічних наук у діяльності Інститут кібернетики імені В.М.Глушкова Національної академії наук України

Даний акт складено про те, що результати дисертаційної роботи Давиденко Анатолія Миколайовича «Методи та моделі функціонування адаптивних засобів захисту доступу до інформаційних систем» 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 запропоновано нову технологію функціонування засобів захисту, що є здатною визначати величини реально існуючих небезпек та атак, що дозволяє оперативно міняти величину міри забезпечення безпечного функціонування системи доступу в залежності від активності зовнішніх небезпек.

Таким чином, результати, отримані Давиденко А.М. при написанні дисертації, дозволили розробити метод адаптації системи доступу, що дозволяє оперативно міняти величину міри забезпечення безпечного функціонування системи доступу 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

Генеральний директор
ТОВ «СОФТЛАЙН ІТ»

_____ Є.П. Гармаш

«03» грудня 2018 р.

АКТ

впровадження результатів роботи Давиденко Анатолія Миколайовича «Побудова типової моделі інтранет-систем для аналізу задач безпеки» **при проведенні експертизи інформаційно-телекомунікаційної системи «Автоматизована система класу 2 для підготовки даних», що розгортається в Департаменті військово-технічної політики, розвитку озброєння та військової техніки Міністерства оборони України.**

Даний акт складено про те, що результати роботи Давиденко Анатолія Миколайовича «Побудова типової моделі інтранет-систем для аналізу задач безпеки» впроваджено та використано у діяльності ТОВ «СОФТЛАЙН ІТ» при проведенні первинної державної експертизи комплексної системи захисту інформації інформаційно-телекомунікаційної системи «Автоматизована система класу 2 для підготовки даних», що розгортається в Департаменті військово-технічної політики, розвитку озброєння та військової техніки Міністерства оборони України.

Автором було запропоновано типову модель загроз безпеці інформації, яка була застосована при розробці моделі загроз безпеці інформації інформаційно-телекомунікаційної системи «Автоматизована система класу 2 для підготовки даних», що розгортається в Департаменті військово-технічної політики, розвитку озброєння та військової техніки Міністерства оборони України.

Таким чином, результати, отримані Давиденко А.М. при написанні, дозволили суттєво знізити час проведення експертизи інформаційно-телекомунікаційної системи «Автоматизована система класу 2 для підготовки даних», що розгортається в Департаменті військово-технічної політики, розвитку озброєння та військової техніки Міністерства оборони України.

Головний спеціалист зі створення КСЗІ
ТОВ «СОФТЛАЙН ІТ» – О.М. Коротун

ЗАТВЕРДЖУЮ
Декан факультету радіофізики,
електроніки та комп'ютерних
систем Київського національного
університету ім. Тараса Шевченка

І.О. Анісімов

11 2019 р.

А К Т

про впровадження результатів дисертаційних досліджень співробітників тематичної групи «Моделювання систем захисту інформації в енергетиці» відділу № 6 Математичного та економетричного моделювання Інституту проблем моделювання ім. Г.Є. Пухова НАН України Давиденка Анатолія Миколайовича, Гільгурта Сергія Яковича та Шабана Максима Радуйовича

Даний акт складено про те, що результати дисертаційних робіт співробітників тематичної групи «Моделювання систем захисту інформації в енергетиці» відділу № 6 Математичного та економетричного моделювання Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України Давиденка Анатолія Миколайовича, Гільгурта Сергія Яковича та Шабана Максима Радуйовича впроваджено у навчальний процес Кафедри радіотехніки та радіоелектронних систем Факультету радіофізики, електроніки та комп'ютерних систем Київського національного університету ім. Тараса Шевченка.

Авторами були розроблені лекції для навчальної дісципліни «Випробування та експертиза засобів захисту інформації», які використовують науково-практичні результати, що отримані Давиденко А.М., Гільгуртом С.Я. та Шабаном М.Р., а саме: методи опису та аналізу критичної інформації на основі використання штучних нейроних мереж, моделі параметрів функціонального профілю захисту в комп'ютерних системах, принципи побудови систем підтримки прийняття рішень орієнтованих на інформаційне забезпечення процедур аналізу кібербезпеки, а також методи створення та аналізу реконіфгуровних засобів захисту інформації на базі ПЛІС.

Завідувач кафедри радіотехніки
та радіоелектронних систем
Київського національного університету
імені Тараса Шевченка
к. т. н., доцент М.І. Рєзніков

ЗАТВЕРДЖУЮ

Генеральний директор
ТОВ «СОФТЛАЙН ІТ»
_____ Є.П. Гармаш
«16» грудня 2019 г.

АКТ

впровадження результатів роботи співробітників тематичної групи «Моделювання систем захисту інформації в енергетиці» відділу № 6 Математичного та економетричного моделювання Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України при проведенні експертизи КСЗІ автоматизованої системи для обробки відкритої інформації Центрального науково-дослідного інституту озброєння та військової техніки Збройних Сил України.

Даний акт складено про те, що результати роботи співробітників тематичної групи «Моделювання систем захисту інформації в енергетиці» відділу № 6 Математичного та економетричного моделювання Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України Давиденка Анатолія Миколайовича, Гільгурта Сергія Яковича та Шабана Максима Радуйовича впроваджено та використано у діяльності ТОВ «СОФТЛАЙН ІТ» при проведенні первинної державної експертизи КСЗІ автоматизованої системи для обробки відкритої інформації Центрального науково-дослідного інституту озброєння та військової техніки Збройних Сил України.

Авторами були запропоновані методи опису та аналізу критичної інформації, які були застосовані при розробці моделі загроз безпеці інформації в автоматизованій системі для обробки відкритої інформації Центрального науково-дослідного інституту озброєння та військової техніки Збройних Сил України.

Таким чином, результати, отримані Давиденко А.М., Гільгуртом С.Я. та Шабаном М.Р., дозволили суттево знизити час проведення експертизи КСЗІ автоматизованої системи для обробки відкритої інформації Центрального науково-дослідного інституту озброєння та військової техніки Збройних Сил України.

Головний спеціалист зі створення КСЗІ
ТОВ «СОФТЛАЙН ІТ» _____ Ю.М. Коротун

«ЗАТВЕРДЖУЮ»
Директор НДЦ «Нафтогазбурмаш»
_____ О.І. Політучий
«30» 12 2019 р.

А К Т

впровадження результатів науково-дослідної роботи «Програмно-технічний комплекс керування технологічним процесом зневоднення бішофіту (шифр БАСК)», що виконувалась згідно результатів загальноакадемічного конкурсу науково-технічних проектів, розпорядження Президії НАН України від 07.03.2019 № 157 та договору від 01 квітня 2019 р. № 23/212-19.

Даний акт складено про те, що результати науково-дослідної роботи «Програмно-технічний комплекс керування технологічним процесом зневоднення бішофіту (шифр БАСК)» впроваджено та використано у діяльності НДЦ «Нафтогазбурмаш» (м. Полтава) при створенні технологічної установки отримання чешуірованого бішофіту $MgCl_2 \cdot 6H_2O$ з хлормагнієвих розсолів. Область застосування – підприємства хімічної промисловості.

Створений в процесі виконання науково-дослідної роботи програмно-технічний комплекс призначений для контролю, оптимізації та управління технологічним процесом видобутку сухого хлориду магнію (бішофіту) шляхом його випарювання з водного розчину і дозволяє підвищити енергетичну та ресурсну ефективність технологічного процесу, а також знизити рівень аварійності.

Впровадження результатів дослідження дозволяє скоротити технологічний ланцюг за рахунок ускладнення алгоритму керування, який здійснюється за допомогою програмно-технічного комплексу на базі програмованого логічного контролеру. В результаті зменшується кількість використаного обладнання, знижується споживання електроенергії, а також підвищується якість кінцевого продукту.

Крім економічних здобутків впровадження результатів науково-дослідної роботи надає також важливі еколого-соціальні переваги. Використання програмованого логічного контролера за рахунок більш точного управління технологічним процесом дозволяє уникнути критичних режимів роботи обладнання, при яких можливий викид хлору, що істотно знижує ризик шкідливого впливу виробництва бішофіту на навколишнє середовище.

Заступник директора
НДЦ «Нафтогазбурмаш» Ткаченко М.М.

Атестати відповідності

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

СИСТЕМА ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

АТЕСТАТ ВІДПОВІДНОСТІ

Зареєстровано в Адміністрації
Державної служби спеціального зв'язку
та захисту інформації України
« 13 » грудня 2013 р. за № 9435
Дійсний до « 13 » грудня 2018 р.

Державна служба спеціального зв'язку
назва державного органа (організації, підприємства, установи), який видав Атестат

та захисту інформації України

засвідчує, що комплексна система захисту інформації

Центру реєстрації віртуальних організацій
назва ІТС

української національної грід-інфраструктури

Київського національного університету імені Тараса Шевченка,

що належить **Київському національному університету**
назва державного органа (організації, підприємства, установи), який є

імені Тараса Шевченка,
власником (розпорядником) ІТС, та його адреса

03680, м. Київ, проспект Академіка Глушкова, 4д,

забезпечує захист інформації відповідно до вимог нормативних документів системи технічного захисту інформації в Україні.

Атестат видано на підставі Експертного висновку, який надано організатором експертизи – Інститутом проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України
назва державного органа (організації, підприємства, установи), який є організатором експертизи

Експертний висновок додається до цього Атестата та є його невід'ємною частиною.

Склад підсистем комплексної системи захисту інформації та вимоги до умов експлуатації об'єкта експертизи визначено у відповідному розділі Експертного висновку.

Заступник Голови Служби _____ **О.В. Корнейко**
м.п. підпис ініціали, прізвище

Держзнак. ПК «Україна». Зам. 3-3246. 2013 р. II кв.

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

СИСТЕМА ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

АТЕСТАТ ВІДПОВІДНОСТІ

Зареєстровано в Адміністрації
Державної служби спеціального зв'язку
та захисту інформації України
« 13 » грудня 2013 р. за № 9434
Дійсний до « 13 » грудня 2018 р.

Державна служба спеціального зв'язку
назва державного органа (організації, підприємства, установи), який видав Атестат

та захисту інформації України

засвідчує, що комплексна система захисту інформації

українського академічного грід-вузла
назва ІТС

Інституту теоретичної фізики ім. М.М. Боголюбова

НАН України,

що належить **Інституту теоретичної фізики**
назва державного органа (організації, підприємства, установи), який є

ім. М.М. Боголюбова НАН України,
власником (розпорядником) ІТС, та його адреса

м. Київ, вул. Метрологічна, 14-б,

забезпечує захист інформації відповідно до вимог нормативних документів системи технічного захисту інформації в Україні.

Атестат видано на підставі Експертного висновку, який надано організатором експертизи – Інститутом проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України
назва державного органа (організації, підприємства, установи), який є організатором експертизи

Експертний висновок додається до цього Атестата та є його невід'ємною частиною.

Склад підсистем комплексної системи захисту інформації та вимоги до умов експлуатації об'єкта експертизи визначено у відповідному розділі Експертного висновку.

Заступник Голови Служби м.п. підпис **О.В. Корнейко** ініціали, прізвище

Держзнак. ПК «Україна». Зам. 3-3246. 2013 р. II кв.

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

СИСТЕМА ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

АТЕСТАТ ВІДПОВІДНОСТІ

Зареєстровано в Адміністрації
Державної служби спеціального зв'язку
та захисту інформації України
«29» грудня 2014 р. за № 11800
Дійсний до «29» грудня 2019 р.

Державна служба спеціального зв'язку
назва державного органа (організації, підприємства, установи), який видав Атестат

та захисту інформації України

засвідчує, що комплексна система захисту інформації

автоматизованої інформаційної системи
назва ІТС

Президії Національної академії наук України,

що належить **Національній академії наук України,**
назва державного органа (організації, підприємства, установи), який є

м. Київ, вул. Володимирська, 54,
власником (розпорядником) ІТС, та його адреса

забезпечує захист інформації відповідно до вимог нормативних документів системи технічного захисту інформації в Україні.

Атестат видано на підставі Експертного висновку, який надано організатором експертизи – Інститутом проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України
назва державного органа (організації, підприємства, установи), який є організатором експертизи

Експертний висновок додається до цього Атестата та є його невід'ємною частиною.

Склад підсистем комплексної системи захисту інформації та вимоги до умов експлуатації об'єкта експертизи визначено у відповідному розділі Експертного висновку.

Перший заступник Голови Служби м.п. підпис **О.В. Корнейко** ініціали, прізвище

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

СИСТЕМА ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

АТЕСТАТ ВІДПОВІДНОСТІ

Зареєстровано в Адміністрації
Державної служби спеціального зв'язку
та захисту інформації України
«29» грудня 2016 р. за № 14650
Дійсний до «29» грудня 2021 р.

Державна служба спеціального зв'язку

назва державного органа (організації, підприємства, установи), який видав Атестат

та захисту інформації України

засвідчує, що комплексна система захисту інформації

автоматизованої системи класу «2» Ресурсного центру Інституту кібернетики Національної академії наук України,

назва ІТС

яка належить **Інституту кібернетики ім. М.В. Глушкова Національної академії наук України ,**

назва державного органа (організації, підприємства, установи), який є

м. Київ, просп. Академіка Глушкова, 40,

власником (розпорядником) ІТС, та його адреса

забезпечує захист інформації, відповідно до вимог нормативних документів системи технічного захисту інформації в Україні.

Атестат видано на підставі Експертного висновку, який надано організатором експертизи –

Інститутом проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України.

назва державного органа (організації, підприємства, установи), який є організатором експертизи

Експертний висновок додається до цього Атестата та є його невід'ємною частиною.

Програмно-апаратний склад автоматизованої системи та вимоги до умов експлуатації об'єкта експертизи зазначені у відповідних розділах Експертного висновку.

Перший заступник Голови Служби _____ **О.М. Чаузов**

підпис ініціали, прізвище

м.п.

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

СИСТЕМА ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

АТЕСТАТ ВІДПОВІДНОСТІ

Зареєстровано в Адміністрації
Державної служби спеціального зв'язку
та захисту інформації України
«27» січня 2017 р. за № 14757
Дійсний до «27» січня 2022 р.

Державна служба спеціального зв'язку
назва державного органа (організації, підприємства, установи), який видав Атестат
та захисту інформації України

засвідчує, що комплексна система захисту інформації

локальної обчислювальної мережі Управління справами
назва ІТС
Національної академії наук України,

яка належить **Національній академії наук України,**
назва державного органа (організації, підприємства, установи), який є
м. Київ, вул. Володимирська, 54,
власником (розпорядником) ІТС, та його адреса

забезпечує захист інформації, відповідно до вимог нормативних документів системи технічного захисту інформації в Україні.

Атестат видано на підставі Експертного висновку, який надано організатором експертизи –

Інститутом проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України.
назва державного органа (організації, підприємства, установи), який є організатором експертизи

Експертний висновок додається до цього Атестата та є його невід'ємною частиною.

Програмно-апаратний склад системи та вимоги до умов експлуатації об'єкта експертизи зазначені відповідно в розділах 2 і 8 Експертного висновку.

Перший заступник Голови Служби _____ **О. М. Чаузов**
підпис ініціали, прізвище
М.П.

Зареєстровано в Адміністрації
Державної служби спеціального зв'язку
та захисту інформації України
«07» вересня 2018 р. за № 17407
Дійсний до «07» вересня 2023 р.

АТЕСТАТ ВІДПОВІДНОСТІ

Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України

(найменування державного органу (організації, підприємства, установи, яким надано Атестат)

засвідчує, що комплексна система захисту інформації

автоматизованої системи класу «2» для підготовки даних Департаменту військово-технічної політики, розвитку озброєння та військової техніки Міністерства оборони України,

(назва ІТС)

що належить **Департаменту військово-технічної політики, розвитку озброєння та військової техніки Міністерства оборони України ,**

(найменування державного органу (організації, підприємства, установи), –

м. Київ, просп. Перемоги, 55/2,

власника (розпорядника) ІТС, місцезнаходження)

забезпечує захист інформації відповідно до вимог нормативних документів з технічного захисту інформації.

Організатор експертизи –

Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України

(найменування державного органу (організації, підприємства, установи), що є організатором експертизи)

Експертний висновок на 59 аркушах додається до цього Атестата та є його невід'ємною частиною.

Вимоги до умов експлуатації об'єкта експертизи визначено у відповідному розділі Експертного висновку.

Директор Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України чл.-кор. НАН України підпис **В. В. Мохор** ініціали, прізвище

Зареєстровано в Адміністрації
Державної служби спеціального зв'язку
та захисту інформації України
«8» травня 2019 р. за № 19159
Дійсний до «8» травня 2024 р.

АТЕСТАТ ВІДПОВІДНОСТІ

Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України

(найменування державного органу (організації, підприємства, установи, яким надано Атестат)

засвідчує, що комплексна система захисту інформації **Автоматизованої системи для обробки відкритої інформації Центрального науково-дослідного інституту озброєння та військової техніки Збройних Сил України,**

(назва ІТС)

що належить **Центральному науково-дослідного інституту озброєння та військової техніки Збройних Сил України**

(найменування державного органу (організації, підприємства, установи), –

м. Київ, Повітрофлотський проспект, 28,

власника (розпорядника) ІТС, місцезнаходження)

забезпечує захист інформації відповідно до вимог нормативних документів з технічного захисту інформації.

Організатор експертизи –

Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України.

(найменування державного органу (організації, підприємства, установи), що є організатором експертизи)

Експертний висновок на 66 аркушах додається до цього Атестата та є його невід'ємною частиною.

Вимоги до умов експлуатації об'єкта експертизи визначено у відповідному розділі Експертного висновку.

Директор Інституту проблем моделювання в енергетиці ім. Г.Є. Петухова НАН України чл.-кор. НАН України _____ **В.В. Мохор**

підпис ініціали, прізвище

Рекомендаційний лист

LUNDS UNIVERSITET

Pukhov Institute for Modelling
in Energy Engineering
National Academy of Sciences of Ukraine
15, General Naumov Str.
03164, Kyiv, Ukraine

Recommendation letter

The series of scientific research works devoted to the grid and cloud services development authored by Anatolii Davydenko (Pukhov Institute for Modeling in Energy Engineering, Kyiv, Ukraine; davidenkoan@gmail.com), Serhii Hilhurt (Pukhov Institute for Modeling in Energy Engineering, Kyiv, Ukraine; hilgurt@ipme.kiev.ua) and Andrii Salnikov (National Taras Shevchenko University of Kyiv, Ukraine; manf@grid.org.ua) is well known by the NorduGrid international community as it was presented on the series of annual NorduGrid Conferences.

In particular, the report "Web-service for FPGA synthesis using ARC-powered grid infrastructure" (https://indico.lucas.lu.se/event/573/session/8/contribution/9) took a worthy place among proceedings of the annual NorduGrid Conference "From Data Factories to Insight as a Service" that took place in Tromsø, Norway on 28-30 June 2017.

In general, the work of the team is of undoubted interest for the e-Science community as a basis for building services of such type. I had discussed the results of this work with the authors and recommend to support further development in this area in Ukraine.

Dr. Balázs Kónya 5/3/2019 LUND

Technical Coordinator
NorduGrid Collaboration
www.nordugrid.org

Lund University
Department of Physics
BOX 118, S - 221 00 LUND,
Sweden

balazs.konya@hep.lu.se
phone: +46 46 222 8049
fax: +46 46 222 4015

Акт здачі-приймання наукової роботи

Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України

НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

АКТ № 1
від 28 грудня 2019 р.
здачі-приймання наукової роботи

„Підтримка грід-сайту ІПМЕ ім. Г.Є. Пухова НАН України та модернізація веб-сервісу централізованого програмування реконфігуровних засобів інформаційної безпеки на базі гріду та хмарної інфраструктури”

виконаної відповідно до Програми інформатизації НАН України на 2019 рік, розпорядження Президії НАН України від 15.03.2019 № 170 «Про затвердження переліку проектів Програми інформатизації НАН України на 2019 рік» та договору від 29 березня 2019 р. № 213-19

Термін виконання роботи : початок 29 березня 2019 р. закінчення 28 грудня 2019 р.

Ми, що нижче підписалися, представник від УСТАНОВИ-ВИКОНАВЦЯ в особі директора Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України члена-кореспондента НАН України Мохора Володимира Володимировича, який діє на підставі Статуту установи з одного боку, та представник від НАН України Перший віце-президент НАН України академік НАН України Наумовець Антон Григорович, який діє на підставі розпорядження Президії НАН України від 15.03.2019 № 170 «Про затвердження переліку проектів Програми інформатизації НАН України на 2019 рік» з іншого боку, склали цей акт про те, що наукова робота задовольняє умовам технічного завдання.

Стислий зміст проведеної роботи та одержані результати:

Забезпечено належний рівень показників надійності та доступності грід-сайту UA-PIMEE та ВО MatModEn в інфраструктурах УНГ і EGI; модернізовано веб-сервіс універсальної (на базі гріду та хмарних обчислень) системи централізованого програмування реконфігуровних прискорювачів, що застосовуються для вирішення задач інформаційної безпеки в енергетичній галузі з метою підвищення її функціональних характеристик, а саме – розроблені методи створення ефективних структур сигнатурного розпізнавання, розроблені нові алгоритми її використання, проведене експериментальне підтвердження здобутих результатів.

Звіт про виконання науково-технічного проєкту схвалено на засіданні Вченої ради Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, (протокол від 31 жовтня 2019 р. № 12)

Додатки, що є невід'ємною частиною акта здачі-приймання наукової роботи:

1. Кошторис витрат (Додаток А) з розрахунками витрат за статтями.
2. Перелік статей накладних витрат (Додаток Б).
3. Звіт про виконання наукової роботи із зазначенням № протоколу та дати засідання вченої ради установи зі списком публікацій за результатами виконання роботи у звітному році;

Плановий кошторис витрат на 2019 р. складає 70,00 тис. грн.
Сімдесят тисяч гривень
(*сума прописом*)
Загальна сума виділених асигнувань 70,00 тис. грн.
Сімдесят тисяч гривень
(*сума прописом*)
Загальний обсяг виконаних робіт 70,00 тис. грн.
Сімдесят тисяч гривень
(*сума прописом*)
Загальний обсяг оплачених робіт (касові видатки) 70,00 тис. грн.
Сімдесят тисяч гривень
(*сума прописом*)
Підлягає до перерахування установі-виконавцю 0,0 тис. грн.
Нуль гривень
(*сума прописом*)

Роботу здав:

УСТАНОВА-ВИКОНАВЕЦЬ
Директор Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, член-кореспондент НАН України

_____ **В.В. Мохор**
(*підпис*)
М.П.

Науковий керівник роботи
член-кореспондент НАН України

_____ В.Ф. Євдокимов
(*підпис*)

Начальник планово-економічного відділу

_____ В.І. Павловська
(*підпис*)

Головний бухгалтер

_____ Г.В. Степанищенко
(*підпис*)

Роботу прийняв:

НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
Перший віце-президент НАН України,
Академік НАН України

_____ **А.І. Наумовець**
(*підпис*)
М.П.

Начальник Відділу фінансово-економічного забезпечення діяльності НАН України

_____ **Л.С. Литвишко**
(*підпис*)

ДОДАТОК Б. ЛІСТИНГ РОЗРОБЛЕНИХ ПРОГРАМНИХ ЗАСТОСУНКІВ БЕЗПЕКИ СИСТЕМ РОЗМЕЖУВАННЯ ДОСТУПУ

Програмне забезпечення грід-сервісу STRAGS віддаленого синтезу конфігурацій для реконфігуровних засобів захисту інформації

Програмна реалізація грід-сервісу

Веб-сервіс. Компоненти веб-сервісу виконані мовою програмування PHP, використовують веб-сервер Apache та базу даних MySQL. Apache налаштований на авторизацію по персональним сертифікатам користувачів, результати якої обробляються в PHP.

Для запуску завдань-агентів використовуються SHELL-сценарії, що для взаємодії з грід-інфраструктурою викликають бінарні клієнти Nordugrid ARC.

API реалізовано за допомогою REST-підходу з використанням семантики JSON.

Веб-інтерфейс користувача. Веб інтерфейс створено за допомогою використання стилів Twitter Bootstrap та бібліотек jQuery для здійснення AJAX запитів в JSON API веб-серверу.

Агент STRAGS. Створена віртуальна машина працює під керування ОС Scientific Linux 6.7 на яку встановлено фірмовий програмний пакет САПР Xilinx WebPACK ISE ver.10.1 та всі необхідні програмні компоненти для його роботи.

Реалізацію компонентів агенту виконано мовою Python, включаючи клієнт JSON API та всі операції взаємодії з сервером. Обробник завдань виконано як SHELL-сценарій що викликає команди наперед встановленого програмного забезпечення для моделювання конфігурації ПЛІС.

Лістинг деяких компонентів программного забезпечення грід-сервісу STRAGS віддаленого синтезу конфігурацій для реконфігуровних засобів захисту інформації:

Модуль ініціювання грід-завдання **jobsubmit.php** (мовою PHP)

```
<?php
require("init.php");
function send_response($code,$msg) {
  $result['status'] = $code;
  $result['status_info'] = $msg;
```

```
  echo json_encode($result);
  exit(0);
}
// HTTPS auth first
$auth = new AuthHTTPS();
if ( ! $auth->isAuthenticated() ) {
   send_response(10, 'User is not authenticated. Make sure you have imported your grid-certificate into
the browser');
}
$user = $auth->getDN();
$dbuser = DB::QueryResultValue("SELECT id FROM users WHERE dn = ?(user)", $user);
if (is_null($dbuser)) {
   $dbuser = DB::InsertQuery("INSERT INTO users(dn) VALUES (?(user))", $user);
}
// Process form submission
if(isset($_POST["submit"])){
   if ( ! isset($_POST["jobname"]) ) {
     send_response(20,'Job name is required for new job');
   }
   $jobname = $_POST["jobname"];
   if ( empty($jobname) ) send_response(21,'Job name is required for new job');
   // get project archive
   $projarch = $_FILES["projarch"]["tmp_name"];
   $projmd5 = md5_file($projarch);
   // copy to filestore
   $fstore_path = FILESTORE_PATH . '/' . substr($projmd5,0,1) . '/' . substr($projmd5,0,2) . '/';
   if ( ! is_dir($fstore_path) ) mkdir($fstore_path, 0700, true);
   move_uploaded_file($projarch, $fstore_path . $projmd5);
   // register new job in database
   DB::InsertQuery("INSERT INTO jobs(`name`,`project`,`user`,`submitted`) " .
               "VALUES (?(jobname), ?(projmd5), ?(dbuser), CURRENT_TIMESTAMP)",
               $jobname, $projmd5, $dbuser);
} else {
   send_response(30, 'There is no job submission data');
}
 send_response(0, 'OK');
?>
```

Модуль запуску грід-агента **agentrun.php** (мовою PHP)

```
<?php
require("init.php");
date_default_timezone_set('Europe/Kiev');
if ( php_sapi_name() != 'cli' ) {
  $auth = new AuthHTTPS();
  if ( ! is_admin($auth->getDN()) ) {
        Logger::Error("You are not allowed to control job submission");
        exit(0);
  }
} else {
  // parse command line arguments (for direct submission)
  if ( isset($argv[1]) ) {
```

```
        if ( $argv[1] == 'grid' ) {
                define('GRID_FORCE_SUBMISSION', TRUE);
                Logger::Info("Direct submission of grid agent is requested.");
        }
        if ( $argv[1] == 'amazon' ) {
                define('AWS_SUBMISSION', TRUE);
                Logger::Info("Amazon EC2 agent submission is requested.");
        }
  }
}
Logger::Info("Starting agent submission cycle at " . date("Y-m-d H:i:s"));
// Get number of available agents
$stadby_agents = DB::QueryResultValue('SELECT COUNT(`agent_key`) FROM `agents` WHERE
`status` = 1');
if ( is_null($stadby_agents) ) {
   $stadby_agents = 0;
}
if (!defined('GRID_FORCE_SUBMISSION') and !defined('AWS_SUBMISSION')) {
 // Get configured agents number
 $configured_standby_agents = DB::QueryResultValue('SELECT `value` FROM `settings` WHERE
`name` = "standby_agents"');
 if ( is_null($configured_standby_agents) ) {
    $configured_standby_agents = 2;
 }
 if ( $stadby_agents > $configured_standby_agents ) {
   Logger::Info("There are already $stadby_agents agents in standby ($configured_standby_agents
configured). Skipping submission");
   exit(0);
 }
}
Logger::Info("Submitting new agent ($stadby_agents agents in standby)");
// Generate UUID
$agent_uuid = DB::QueryResultValue("SELECT UUID()");
Logger::Debug("Agent UUID $agent_uuid");
// Add UUID to database
DB::InsertQuery("INSERT INTO agents(`agent_key`) VALUE (?(agent_uuid))", $agent_uuid);
// Run agent
$agentjobdir = STRAGS_ROOT_ . "jobs/agents/" . $agent_uuid ;
$shell_cmd = STRAGS_ROOT_ . "helpers/submitwrap.sh " . $agentjobdir . " " . $agent_uuid;
if (defined('AWS_SUBMISSION')){
 $shell_cmd = $shell_cmd . " amazon";
}
$exit_code = 1;
passthru("$shell_cmd", $exit_code);

Logger::Info("Agent submission finished with exit code $exit_code");
if ( $exit_code == 0 ) {
 $agentlocation = file_get_contents("$agentjobdir/job.location");
 Logger::Info("Agent submitted to $agentlocation");
```

```
  DB::UpdateQuery('UPDATE `agents` SET `location` = ?(agentlocation) WHERE `agent_key` =
?(agent_uuid)',$agentlocation, $agent_uuid);
  if (defined('AWS_SUBMISSION')){
     // define special state to reflect instance was created on EC2
     DB::UpdateQuery('UPDATE `agents` SET `status` = 5 WHERE `agent_key` = ?(agent_uuid)',
$agent_uuid);
  }
}
?>
```

Модуль видалення грід-агента **agentcleanup.php** (мовою PHP)

```
<?php
require("init.php");
date_default_timezone_set('Europe/Kiev');
if ( php_sapi_name() != 'cli' ) {
   $auth = new AuthHTTPS();
   if ( ! is_admin($auth->getDN()) ) {
         Logger::Error("You are not allowed to control job submission");
         exit(0);
   }
}
// Do not trigger most cleanups often that hourly
$state_file = '/tmp/strags-agents-cleanup.state';
$do_hourly = FALSE;
if (file_exists($state_file)) {
   if (time() - filemtime($state_file) >= 3600) {
         $do_hourly = TRUE;
   }
} else {
   $do_hourly = TRUE;
}

if ( $do_hourly ) {
  Logger::Info("Starting agent complete cleanup cycle at " . date("Y-m-d H:i:s"));
  // Remove agents not started during 1 day
  Logger::Info("Removing agents that failed to start in 24 hours");
  DB::UpdateQuery('DELETE FROM `agents` WHERE `status` = 0 AND `status_timestamp` <
DATE_SUB(NOW(), INTERVAL 1 DAY)');
  // Move lost agents to unreachable state (no heartbeat within 30 minutes)
  Logger::Info("Marking agents that failed to send heartbeat in 30 minutes as unreachable");
  DB::UpdateQuery('UPDATE `agents` SET `status` = 0 WHERE `status` in (1,2) AND
`status_timestamp` < DATE_SUB(NOW(), INTERVAL 30 MINUTE)');
  // cleanup obsolete agent state diretories
  function rrmdir($dir) {
    if (is_dir($dir)) {
      $objects = scandir($dir);
      foreach ($objects as $object) {
        if ($object != "." && $object != "..") {
          if (is_dir($dir."/".$object))
            rrmdir($dir."/".$object);
          else
```

```
            unlink($dir."/".$object);
          }
        }
        rmdir($dir);
      }
    }
    Logger::Info("Cleaning obsolete agents directories");
    $agents_arr = DB::QueryAllResultValues('SELECT `agent_key` FROM `agents`');
    $agents_dirs = scandir(STRAGS_ROOT_ . "jobs/agents/");
    foreach ( $agents_dirs as $dir ) {
      if ( $dir == 'ssh' || $dir == 'ssh-key' ) continue;
      if ( $dir == '.' || $dir == '..' ) continue;
      if (! in_array($dir, $agents_arr) ) {
          Logger::Debug("Removing agent ". $dir . " state directory");
          rrmdir(STRAGS_ROOT_ . "jobs/agents/" . $dir);
      }
    }
    touch($state_file);
}
// Handle terminating agents
$terminating_agents = DB::QueryAllResultValues('SELECT `agent_key` FROM `agents` WHERE
`status` = 6');
if(!empty($terminating_agents)) {
  foreach ( $terminating_agents as $agent_uuid ) {
    Logger::Info("Checking that agent " . $agent_uuid . " ia already terminated.");
    $agentjobdir = STRAGS_ROOT_ . "jobs/agents/" . $agent_uuid;
    $shell_cmd = STRAGS_ROOT_ . "helpers/check_terminated.sh \"" . $agentjobdir . "\"";
    $exit_code = 1;
    passthru($shell_cmd, $exit_code);
    if ( $exit_code == 0 ) {
          Logger::Info("Agent " . $agent_uuid . " had finished terminating. Updating status.");
        DB::UpdateQuery('UPDATE `agents` SET `status` = 0 WHERE `agent_key` = ?(agent_uuid)',
$agent_uuid);
    }
  }
}

?>
```

Модуль контролера грід-завданнь **jobcntl.php** (мовою PHP)

```
<?php
require("init.php");
$result = array ();
function send_response ($return_code, $return_string) {
  global $result;
  // add request processing status to JSON answer
  $result['status'] = $return_code;
  $result['status_info'] = $return_string;
  echo json_encode($result);
  exit(0);
}
```

```
// HTTPS auth first
$auth = new AuthHTTPS();
if ( $auth->isAuthenticated() ) {
  $user = $auth->getDN();
  $dbuser = DB::QueryResultValue("SELECT id FROM users WHERE dn = ?(user)", $user);
  if (is_null($dbuser)) {
    $dbuser = DB::InsertQuery("INSERT INTO users(dn) VALUES (?(user))", $user);
  }
  $result['auth'] = $user;
} else {
  $result['auth'] = 0;
  send_response(10, 'User is not authenticated. Make sure you have imported your grid-certificate into
the browser');
}
// Action
$action = isset($_GET['action']) ? $_GET['action'] : 'resubmit';
// Job ID is required
if ( isset($_GET['jobid']) && is_numeric($_GET['jobid']) ) {
  $jobid = $_GET['jobid'];
} else {
  send_response(21, 'Job ID is not defined.');
}
if ( $action == 'resubmit' ) {
  $resub_res = DB::UpdateQuery('UPDATE jobs SET `status` = 0, `progress` = 0,
                                `progress_info` = "Resubmitted"
                            WHERE `id` = ?(jobid) AND `user` = ?(dbuser)',
                                $jobid, $dbuser);
  if ( ! $resub_res ) {
    send_response(31, 'Failed to resubmit job.');
  }
} else if ( $action == 'cleanup' ) {
  $clean_res = DB::UpdateQuery('DELETE FROM jobs
                            WHERE `id` = ?(jobid) AND `user` = ?(dbuser)',
                                $jobid, $dbuser);
  if ( ! $clean_res ) {
    send_response(32, 'Failed to cleanup job.');
  }
}
send_response(0, 'OK');
?>
```

Структура бази даних сервісу STRAGS (мовою SQL)

```
CREATE TABLE IF NOT EXISTS `agents` (
  `agent_key` char(36) NOT NULL,
  `status` tinyint(3) unsigned NOT NULL DEFAULT '0',
  `status_timestamp` timestamp NOT NULL DEFAULT CURRENT_TIMESTAMP ON UPDATE
CURRENT_TIMESTAMP,
  PRIMARY KEY (`agent_key`),
  UNIQUE KEY `agent_key` (`agent_key`)
) ENGINE=InnoDB DEFAULT CHARSET=latin1;
CREATE TABLE IF NOT EXISTS `jobs` (
```

```
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `name` varchar(255) CHARACTER SET utf8 NOT NULL,
  `project` char(32) NOT NULL,
  `user` int(11) NOT NULL,
  `submitted` timestamp NULL DEFAULT NULL,
  `status_timestamp` timestamp NOT NULL DEFAULT CURRENT_TIMESTAMP ON UPDATE
CURRENT_TIMESTAMP,
  `status` tinyint(3) unsigned NOT NULL DEFAULT '0',
  `progress` tinyint(3) unsigned NOT NULL DEFAULT '0',
  `progress_info` varchar(64) CHARACTER SET utf8 COLLATE utf8_unicode_ci NOT NULL
DEFAULT 'Accepted',
  PRIMARY KEY (`id`),
  KEY `user` (`user`,`status`)
) ENGINE=InnoDB  DEFAULT CHARSET=latin1;
CREATE TABLE IF NOT EXISTS `settings` (
  `name` char(32) NOT NULL,
  `value` varchar(255) NOT NULL,
  UNIQUE KEY `name` (`name`)
) ENGINE=MyISAM DEFAULT CHARSET=latin1;
CREATE TABLE IF NOT EXISTS `users` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `dn` varchar(255) NOT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB  DEFAULT CHARSET=latin1;
```

Модуль оновлення агентів **run_agent_update.sh** (скриптовою мовою командної оболонки sh)

```
#!/bin/bash
STRAGS_AGENT_TAR="STRAGS.tar.gz"
STRAGS_AGENT_URL="http://strags.matmoden.kiev.ua/vms/${STRAGS_AGENT_TAR}"
STRAGS_UPDATE_TMPDIR=/tmp/strags-update
STRAGS_PATH="/opt/STRAGS"
rm -rf ${STRAGS_UPDATE_TMPDIR}
mkdir -p ${STRAGS_UPDATE_TMPDIR}
cd ${STRAGS_UPDATE_TMPDIR}
wget ${STRAGS_AGENT_URL} -O ${STRAGS_AGENT_TAR}
if [ $? -ne 0 ]; then
  echo "FATAL: Failed to download STRAGS agent updated archive."
  exit 1
fi
tar xf ${STRAGS_AGENT_TAR}
rm -rf "${STRAGS_PATH}.old"
mv "${STRAGS_PATH}" "${STRAGS_PATH}.old"
mv STRAGS "${STRAGS_PATH}"
```

Модуль синтезу проєкту для ПЛІС **run_xilinx.sh** (скриптовою мовою командної оболонки sh)

```
#!/bin/bash
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
LOCKFILE=/mnt/data/agent.lock
EXEC_LOG=execution.log
RULES_FILENAME=rules.txt
```

```
VHD_NAME=MonoLine.vhd
VHD_GENERATOR=/opt/STRAGS/genvhd.sh
parch=$1
jobid=$2
# create log file
touch $EXEC_LOG
exec 1>$EXEC_LOG
exec 2>&1
# lock to compute one job per-agent
[ -f $LOCKFILE ] && exit 0
trap "rm -f $LOCKFILE" EXIT
touch $LOCKFILE
# define some hardcoded models
partname="xc3s500e-fg320-4"
instyle="ise"
#instyle="xflow"
# add Xilinx pathes
source /opt/Xilinx/10.1/ISE/settings32.sh
# progress reporter
progress () {
cat <<END
------------------------------------------------------------
--- $2
------------------------------------------------------------
END
 /opt/STRAGS/StragsReporter.py $jobid $1 "$2" >/dev/null 2>&1
}
# extract project archive
progress 1 'Extracting project archive'
if file $parch | grep -qi 'rar'; then
  unrar e -o+ $parch
  [ $? -ne 0 ] && exit 1
elif file $parch | grep -qi ' zip '; then
  unzip -o $parch
  [ $? -ne 0 ] && exit 1
else
  tar xf $parch
  [ $? -ne 0 ] && exit 1
fi
progress 3 'Preparing working directory'
# .xst is a starting point
jobworkdir=$( pwd )
xst_file=$( find . -name '*.xst' )
xst_dir=${xst_file%/*.xst}
xst_file=${xst_file##*/}
fbase=${xst_file%.xst}
cd $xst_dir
# create defined tmpdir
rm -rf xst
cat $xst_file | sed -n '/set/s/^\s*set\s*-tmpdir\s*//p' | sed 's/\r//' | xargs mkdir -p
```

```
# generating vhd file based on rueles.txt
progress 10 'Running vhd generator'
if [ -f "$RULES_FILENAME" ]; then
   $VHD_GENERATOR "$RULES_FILENAME" "$VHD_NAME"
fi
# run xst
progress 10 'Running xst'
xst -intstyle "$instyle" -ifn "${xst_file}"
[ $? -ne 0 ] && exit 1
# run ngdbuild
progress 15 'Running ngdbuild'
ngdbuild -intstyle "$instyle"  -uc "$( find . -name '*.ucf' )" -p "$partname" "${fbase}.ngc"
"${fbase}.ngd"
[ $? -ne 0 ] && exit 1
# run map
progress 20 'Running map'
map -intstyle "$instyle" -p "$partname" -cm area -pr off -c 100 -o "${fbase}_map.ncd" "${fbase}.ngd"
"${fbase}.pcf"
[ $? -ne 0 ] && exit 1
# run par
par_reportsrt="Running par"
progress 25 "$par_reportsrt"
pi=25
par -intstyle "$instyle" -w -ol high "${fbase}_map.ncd" "${fbase}.ncd" "${fbase}.pcf" | while read
parline; do
  if echo $parline | grep -iq 'Starting Placer'; then
    pi=30
    step=2
    par_reportsrt="Running par (placer)"
    progress $pi "$par_reportsrt"
  elif echo $parline | grep -iq 'Starting Router'; then
    pi=60
    step=2
    par_reportsrt="Running par (router)"
    progress $pi "$par_reportsrt"
  elif echo $parline | grep -iq 'Phase'; then
    pi=$(( pi + step ))
    progress $pi "$par_reportsrt"
  fi
  echo $parline
done
# run bitgen
progress 95 'Running bitgen'
bitgen -intstyle "$instyle" -f "${fbase}.ut" "${fbase}.ncd"
[ $? -ne 0 ] && exit 1
# move result
mv "${fbase}.bit" "${jobworkdir}/result.bit"
[ $? -ne 0 ] && exit 1
cd "${jobworkdir}"
progress 100 'Uploading results'
```

Модуль клієнта JSON API **StragsCommon.py** (мовою Python)

```
#!/usr/bin/python
import os
import sys
import requests
import json
import subprocess
_strags_url = 'https://strags.matmoden.kiev.ua/agentapi.php'
_strags_key_file = '/mnt/data/agent.key'
_strags_ver_file = '/opt/STRAGS/version'
_strags_update = '/opt/STRAGS/run_agent_update.sh'
_strags_postupdate = '/opt/STRAGS/run_postupdate.sh'
def strags_request (data):
  if not os.path.exists(_strags_key_file):
    sys.exit(1)
  keyf = open(_strags_key_file, 'r')
  data['key'] = keyf.read().replace('\n','')
  keyf.close()
  data['agent_version'] = 0
  if os.path.exists(_strags_ver_file):
    verf = open(_strags_ver_file, 'r')
    data['agent_version'] = verf.read().replace('\n','')
    verf.close()
  response = False
  requests.packages.urllib3.disable_warnings()
  r = requests.put(_strags_url, data=json.dumps(data), verify=False)
  if r.status_code == 200:
    response = r.json()
    if not response:
    print 'ERROR: Communication with STRAGS server failed'
    sys.exit(1)
    if response['status'] != 0:
    print 'ERROR: STRAGS server failed to process our request: ' + response['status_info']
    sys.exit(1)
  if 'agent_version' in response:
    if response['agent_version'] > data['agent_version']:
      subprocess.call(_strags_update, shell=True)
  subprocess.call(_strags_postupdate, shell=True)
  return response
```

Модуль керування агентом **StragsJobAgent.py** (мовою Python)

```
#!/usr/bin/python
import StragsCommon
import sys
import os
import base64
import subprocess
_workdir = '/mnt/data/'
_agent_jobfile = '/mnt/data/agent.lock'
_compute_sh = '/opt/STRAGS/run_xilinx.sh'
# exit if still working
```

```
if os.path.exists(_agent_jobfile):
  sys.exit(0)
# get job from STRAGS server
data = {}
data['reqtype'] = 'getjob'
jobinfo = StragsCommon.strags_request(data)
# pass on wait instruction
if jobinfo['action'] == 'wait':
  sys.exit(0)
if jobinfo['action'] != 'process_job':
  print 'ERROR: Unknown action in STRAGS response. It seams you should update agent.'
  sys.exit(1)
# create per-job workdir
jobworkdir = _workdir + str(jobinfo['jobid'])
if not os.path.isdir(jobworkdir):
  os.mkdir(jobworkdir)
os.chdir(jobworkdir)
# fetch project archive
projreq = {}
projreq['reqtype'] = 'getfile'
projreq['fileid'] = jobinfo['projid']
projdata = StragsCommon.strags_request(projreq)
projf = open('project.archive', 'w')
projf.write(base64.b64decode(projdata['data']))
projf.close()
# accept job
acceptjob = {'reqtype': 'acceptjob', 'jobid' : jobinfo['jobid'] }
StragsCommon.strags_request(acceptjob)
# functions to put result files and report failed status
result_path = jobworkdir + '/result.bit'
logs_path = jobworkdir + '/execution.log'
def report_failed (info):
  failreq = {}
  failreq['reqtype'] = 'updatejob'
  failreq['jobid'] = jobinfo['jobid']
  failreq['progress'] = 255
  failreq['progress_info'] = info
  StragsCommon.strags_request(failreq)
  sys.exit(0)
def put_file (fpath, ftype='bit'):
  putreq = {}
  putreq['reqtype'] = 'putresult'
  putreq['fileid'] = jobinfo['projid']
  putreq['jobid'] = jobinfo['jobid']
  putreq['type'] = ftype
  if os.path.exists(fpath):
    putf = open(fpath, 'r')
    putreq['data'] = base64.b64encode(putf.read())
    putf.close()
    StragsCommon.strags_request(putreq)
```

```
  else:
    if ftype == 'log':
      report_failed('General STRAGS agent fault. There is no log file found.')
    else:
      report_failed('There is no ' + ftype + ' file found. See logs for error details.')
# run job (job will report progress to STRAGS itself)
job_cmd = _compute_sh + ' project.archive ' + str(jobinfo['jobid'])
if subprocess.call(job_cmd, shell=True) != 0:
  put_file(logs_path, 'log')
  report_failed('FPGA modeling failed. See logs for details.')
# upload result
put_file(logs_path, 'log')
put_file(result_path)
```

Модуль сповіщення про стан агента **StragsHeartbeat.py** (мовою Python)

```
#!/usr/bin/python
import StragsCommon
import os
_agent_jobfile = '/mnt/data/agent.lock'
data = {}
data['reqtype'] = 'heartbeat'
data['status']  = 2 if os.path.exists(_agent_jobfile) else 1
StragsCommon.strags_request(data)
```

Модуль відображення стану процесу **StragsReporter.py** (мовою Python)

```
#!/usr/bin/python
import StragsCommon
import sys
progress = {}
progress['reqtype'] = 'updatejob'
progress['jobid'] = sys.argv[1]
progress['progress'] = sys.argv[2]
progress['progress_info'] = sys.argv[3] if len(sys.argv) > 3 else ''
StragsCommon.strags_request(progress)
```

Модуль опису стартової сторінки сервісу **index.html** (мовою HTML)

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <meta name="description" content="">
    <meta name="author" content="">
    <title>STRAGS</title>
    <!-- Bootstrap Core CSS -->
    <link href="/ui/css/bootstrap.min.css" rel="stylesheet">
    <!-- Custom CSS -->
    <link href="/ui/css/3-col-portfolio.css" rel="stylesheet">
    <!-- HTML5 Shim and Respond.js IE8 support of HTML5 elements and media queries -->
    <!-- WARNING: Respond.js doesn't work if you view the page via file:// -->
    <!--[if lt IE 9]>
        <script src="https://oss.maxcdn.com/libs/html5shiv/3.7.0/html5shiv.js"></script>
```

```
    <script src="https://oss.maxcdn.com/libs/respond.js/1.4.2/respond.min.js"></script>
  <![endif]-->
        <style type="text/css">
.btn-xlarge {
  padding: 18px 28px;
  font-size: 22px;
  line-height: normal;
  -webkit-border-radius: 8px;
    -moz-border-radius: 8px;
        border-radius: 8px;
  }
                .portfolio-item {
                        margin-bottom: 5px;
                }
                .portfolio-item img {
                        height: 180px;
                         display: block;
                        position: relative;
                        right: 0;
                }
                footer {
                        margin: 50px 0;
                }
        </style>
</head>
<body>
  <!-- Page Content -->
  <div class="container">
    <!-- Page Header -->
    <div class="row">
      <div class="col-lg-12">
        <h3 class="page-header" style="text-align:center; margin:20px auto; "><img
src="/ui/i/logo.png"><br>
          <small>(Security Tasks Reconfigurable Accelerators Grid-Service)</small>
        </h3>
      </div>
    </div>
    <!-- /.row -->
                    <!-- Page Header -->
    <div class="row">
      <div class="col-lg-12">
        <h4 style="color: #337ab7; text-align: center; max-width: 650px; margin: 0
auto;">Централізований синтез файлів конфігурації для реконфігуровних апаратних
прискорювачів задач інформаційної безпеки <i>як сервіс</i></h4>
                <h4 style="text-align: center;"><a href="https://strags.matmoden.kiev.ua/ui/"
class="btn btn-success btn-lg" style="margin: 40px auto;">Розпочати роботу</a></h4>
      </div>
    </div>
    <!-- /.row -->
    <!-- Projects Row -->
```

```
      <div class="row">
        <div class="col-md-4 portfolio-item" style="text-align: right;">
            <img class="img-responsive" src="/ui/i/1_SUME_720x600.jpg" alt="" align="right">
        </div>
                <div class="col-md-4 portfolio-item">
                    <center>
            <img class="img-responsive" src="/ui/i/2_PLIS.jpg" alt="" >
                    </center>
        </div>
                    <div class="col-md-4 portfolio-item">
                    <center>
            <img class="img-responsive" src="/ui/i/3_Altera_Net.jpg" alt="" align="left">
                    </center>
        </div>
      </div>
      <!-- /.row -->
              <h4 style="color: #DEB887; text-align: center; margin: 0 auto;" >З використанням апаратних ресурсів <i>національної грід-інфраструктури України</i> та хмари <i>Amazon EC2</i></h4>
      <hr>
      <!-- Footer -->
      <footer>
        <div class="row">
          <div class="col-lg-12" style="text-align: center;">
            <p>Проект розроблено за фінансової підтримки з боку Цільової комплексної програми наукових досліджень НАН України «Грід-інфраструктура і грід-технології для наукових і науково-прикладних застосувань», 2015, 2016, 2018-2020 рр.</p>
          </div>
        </div>
        <!-- /.row -->
      </footer>
    </div>
    <!-- /.container -->
    <!-- jQuery -->
    <script src="js/jquery.js"></script>
    <!-- Bootstrap Core JavaScript -->
    <script src="js/bootstrap.min.js"></script>
</body>
</html>
```

Модуль опису інтерфейса користувача **ui\index.html** (мовою HTML)

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <!-- The above 3 meta tags *must* come first in the head; any other head content must come *after* these tags -->
    <meta name="description" content="">
    <meta name="author" content="">
```

```
    <title>STRAGS</title>
    <!-- Bootstrap core CSS -->
    <link href="css/bootstrap.min.css" rel="stylesheet">
    <link href="css/font-awesome.min.css" rel="stylesheet">
    <!-- Custom styles for this template -->
    <link href="css/style.css" rel="stylesheet">
    <script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.3/jquery.min.js"></script>
          <script src="dropzone.min.js"></script>
    <script src="js/bootstrap.min.js"></script>
    <!-- Just for debugging purposes. Don't actually copy these 2 lines! -->
    <!--[if lt IE 9]><script src="../../assets/js/ie8-responsive-file-warning.js"></script><![endif]-->
    <script src="js/ie-emulation-modes-warning.js"></script>
             <script src="js/upload.js"></script>
    <!-- HTML5 shim and Respond.js for IE8 support of HTML5 elements and media queries -->
    <!--[if lt IE 9]>
      <script src="https://oss.maxcdn.com/html5shiv/3.7.2/html5shiv.min.js"></script>
      <script src="https://oss.maxcdn.com/respond/1.4.2/respond.min.js"></script>
    <![endif]-->
          <script type="text/javascript" language="javascript"
src="js/jquery.dataTables.min.js"></script>
    <script type="text/javascript" language="javascript" src="js/dataTables.bootstrap.min.js"></script>

  </head>
  <body>
    <div id="loadingspin" class="loadingspin" style="display:none;">
       <img id="img-locadingspin" src="i/loading_gears.gif" alt="Loading"/>
    </div>
    <div class="container">
          <!-- Modal -->
          <div id="myModal" class="modal">
            <div class="modal-dialog" style="width: 900px">
              <!-- Modal content-->
              <div class="modal-content">
                <div class="modal-header">
                     <button type="button" class="close" data-dismiss="modal">&times;</button>
                     <h4 class="modal-title">Modal Header</h4>
                </div>
                <div class="modal-body">
                </div>
                <div class="modal-footer">
                     <button type="button" class="btn btn-default" data-dismiss="modal">Close</button>
                </div>
              </div>
            </div>
          </div>
    </div>
    <nav class="navbar navbar-inverse navbar-fixed-top">
      <div class="container">
        <div class="navbar-header">
```

```
        <button type="button" class="navbar-toggle collapsed" data-toggle="collapse" data-
target="#navbar" aria-expanded="false" aria-controls="navbar">
          <span class="sr-only">Toggle navigation</span>
          <span class="icon-bar"></span>
          <span class="icon-bar"></span>
          <span class="icon-bar"></span>
        </button>
        <a class="navbar-brand" href="/">STRAGS</a>
      </div>
      <div id="navbar" class="collapse navbar-collapse">
        <ul class="nav navbar-nav">
          <li><a href="#add">Add job</a></li>
          <li><a href="#jobs">Active jobs</a></li>
          <li><a href="#finished">Finished jobs</a></li>
          <li><a class='navbar-admin' href="#admin"></a></li>
        </ul>
                    <ul class="nav navbar-nav navbar-right">
        </ul>
      </div><!--/.nav-collapse -->
    </div>
  </nav>
<div class="container">
    <div id="page_data" class="panel">
      <div class="panel-heading">
        <h2 class="panel-title" style="font-size: 20px; text-align: center;"></h2>
      </div>
                  <div id="alerted"></div>
      <div id="file-dropzone" class="panel-body" style="padding-top: 0px;">
                  </div>
  </div> <!-- /container -->
  <!-- Bootstrap core JavaScript
  ================================================== -->
  <!-- Placed at the end of the document so the pages load faster -->
 </body>
</html>
```