МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ДАВИДЕНКО Анатолій Миколайович

УДК 004.056.52:004.056.53:004.75 (043.3)

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

05.13.21 – «Системи захисту інформації»

Автореферат
дисертації на здобуття наукового ступеня
доктора технічних наук

Київ – 2021

Дисертацією є рукопис.
Робота виконана в Інституті проблем моделювання в енергетиці ім. Г. Є. Пухова Національної академії наук України.

Науковий консультант:	доктор технічних наук, професор, лауреат Державної премії України в галузі науки і техніки **Корченко Олександр Григорович,** Національний авіаційний університет, завідувач кафедри безпеки інформаційних технологій.
Офіційні опоненти:	доктор технічних наук, професор, заслужений діяч науки і техніки України, лауреат Державної премії України в галузі науки і техніки **Шелест Михайло Євгенович,** Національний університет «Чернігівська політехніка», професор кафедри кібербезпеки та математичного моделювання; доктор технічних наук, професор, лауреат Державної премії України в галузі науки і техніки **Рибальський Олег Володимирович,** Національна академія внутрішніх справ, головний науковий співробітник науково-дослідної лабораторії «З проблем криміналістичного забезпечення та судової експертології» Навчально-наукового інституту №2; доктор технічних наук, професор **Казакова Надія Феліксівна,** Одеський державний екологічний університет, професор кафедри інформаційних технологій.

Захист відбудеться «13» травня 2021 р. о 13^{00} на засіданні спеціалізованої вченої ради Д 26.062.17 при Національному авіаційному університеті за адресою: 03058, Київ, пр. Любомира Гузара, 1, корпус 11, ауд. 111.

З дисертацією можна ознайомитись в науково-технічній бібліотеці Національного авіаційного університету за адресою: 03058, Київ, пр. Любомира Гузара, 1.

Автореферат розісланий «13» квітня 2021 р.

Учений секретар
спеціалізованої вченої ради
к.т.н., професор Є. Іванченко

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

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.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність та важливість обраної теми дисертації, сформульовано мету і задачі досліджень, окреслено об'єкт та предмет досліджень, визначено наукову новизну, практичну цінність роботи, надано інформацію про структуру дисертації.

У першому розділі розглянуті теоретичні основи використання моделей розмежування доступу у розподілених інформаційних системах, проведено аналіз дослідного зразка спеціалізованої розподіленої інформаційної системи грід-сайту PIMEE ARC в складі Українського національного гріду, визначено параметри й властивості критичні для його використання у задачах, що розв'язуються.

Моделі розмежування доступу необхідні для побудови політик безпеки, спрямованих на забезпечення конфіденційності, цілісності, доступності та спостереженості. Класична класифікація цих моделей передбачає розподіл їх за типами побудови на основі принципів: надання прав; теорії інформації; теорії імовірності.

Системи доступу до інформаційних ресурсів, які розміщені у комп'ютерних мережах, є одним з головних компонентів 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;

– низка 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.

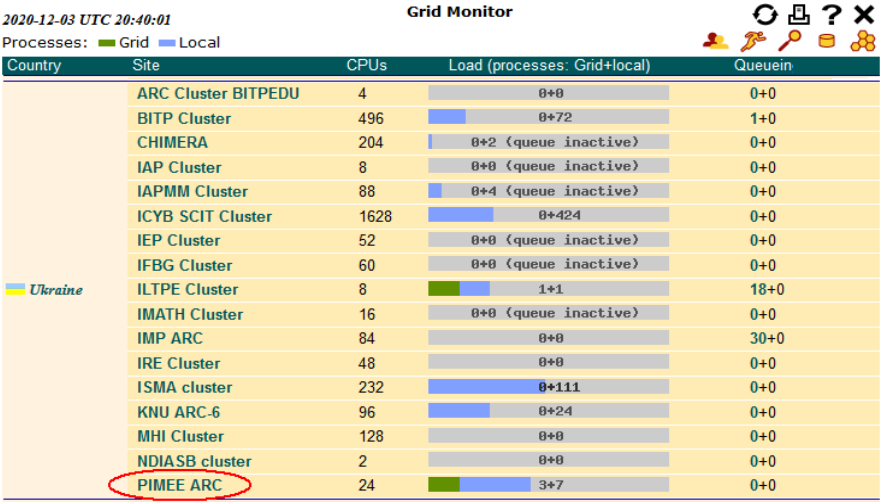
Другим прикладом специфіки роботи системи доступу можуть служити системи, в яких основні функції захисту покладено на процеси й моделі ідентифікації користувачів, які претендують на використання ресурсів. Засоби, які застосовуються для цих цілей, мають досить розвинений апарат криптографії, що ґрунтується на:

– криптографічних алгоритмах;

– протоколах автентифікації;

– низці 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 щодо використання грід-ресурсів під час проведення експериментів (див. рис. 1).



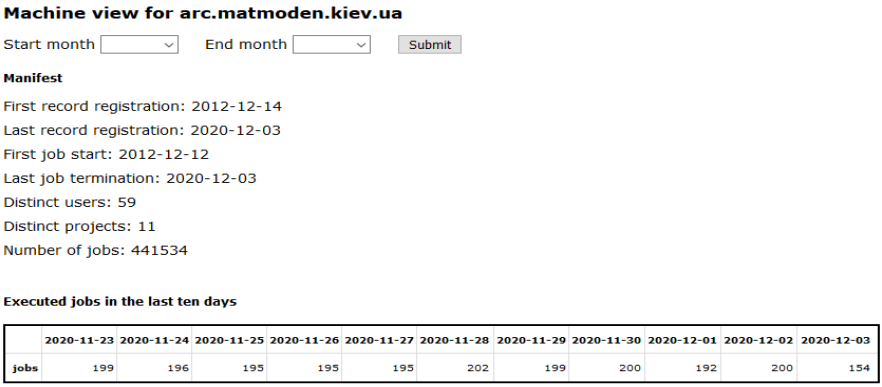
2020-12-03 UTC 20:40:01 — Grid Monitor

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 – 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 репрезентабельність. Наступні дані ілюструють середню завантаженість віртуальної організації matmoden в 200 задач на добу протягом декади (стандартний період моніторингу) згідно даним системи SGAS (див. рис. 2).



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 2 – 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)

Також підтверджена стабільність параметрів протягом року (дані за 2020 рік отримані системою евромоніторинга ARGO, яка є часткою EGI) (див. рис. 3).

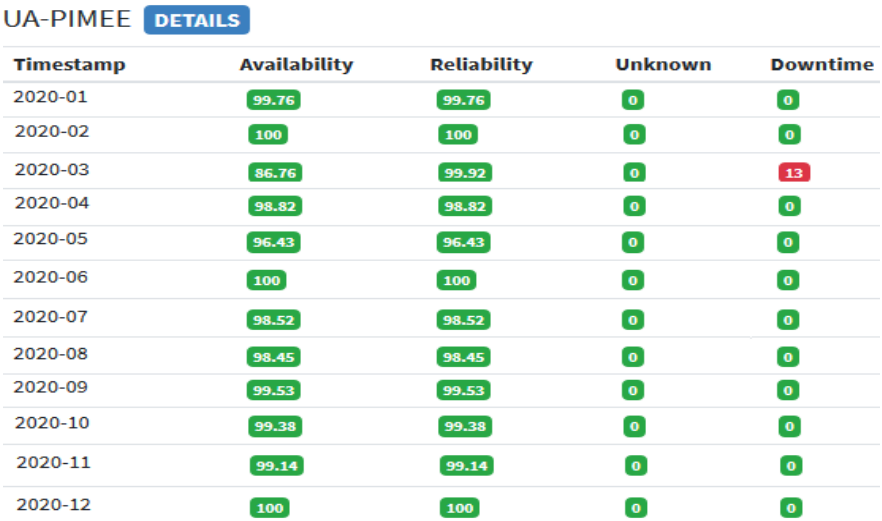


Рисунок 3 – Доступність та надійність грід-сайту ІПМЕ ім. Г.Є. Пухова НАН України за 2020 р. згідно даним системи ARGO (https://argo.egi.eu/egi/report-ar-dates-2/Critical/SITES/UA-PIMEE?start_date=2020-01-01&end_date=2020-12-01)

Таким чином базовими параметрами є стабільне та коректне функціонування дослідного зразка спеціалізованої розподіленої інформаційної системи грід-сайту PIMEE ARC в складі Українського національного гріду, виконуючи 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 в діапазоні 86,76% – 100%. Ці данні є базовими при проведенні експериментів, якщо це не оговорюється окремо.

Проведемо аналіз основних методів розмежування доступу (табл.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 –

Таблиця 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	-	-	-

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.

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 стосовно 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 рис. 4.

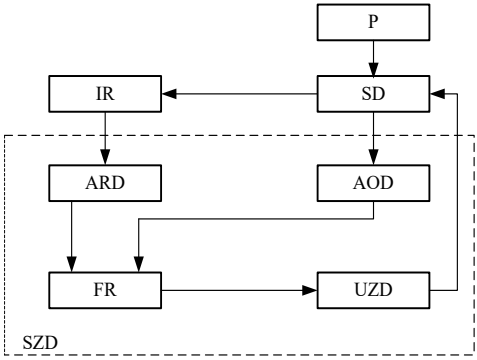


Рисунок 4 – Загальна функціональна схема системи захисту доступу до інформаційних ресурсів

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.

У роботі показано, що для реалізації модулів *ARD* і *AOD* доцільно використовувати нейронні 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. Нейронні мережі в процесі функціонування можуть розвиватися і в процесі такого розвитку формувати нові зразки.

У другому розділі наведені необхідні теоретичні особливості нейронних моделей і обрані узагальнені ознаки класифікації нейронних мереж для їх подальшого аналізу. Оскільки необхідність у реалізації доступу в рамках комп'ютерних мереж досить велика, то й розмаїтість варіантів його реалізації досить широке. 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 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. 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 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 запишемо 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 (ξ^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.

У третьому розділі наведені теоретичні особливості методів навчання нейронних моделей.

Завдання розпізнання нових атак і завдання збільшення ефективності розпізнання атак, яке використовує сигнатури атак, вирішується 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. 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 образу, що розпізнається. 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 ґрунтується 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 керування доступом.

Серед відомих механізмів самоорганізації нейронних систем виділяються два базові підходи до їх реалізації в нейронних мережах різних типів:

– 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.

Підбір ваги вектора w_1 реалізується відповідно до нормалізованих правил 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 η - коефіцієнт навчання. Перша складова відповідає звичайному правилу Хебба, а друга складова реалізує самоорганізацію вагових векторів. Для випадку коли кількість нейронів відповідає кількості складових більш ефективним є правило Сангера, 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 системи 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 ми 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 $x_1(t)$ статично незалежні, то для вирішення проблеми можна використовувати нейронну мережу.

Визначимо схему підключення нейронної мережі (див. рис. 5).

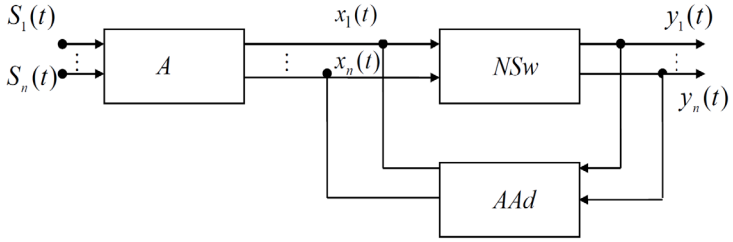


Рисунок 5 – Схема підключення нейронної мережі

де A – матриця змішування; NSw - нейронна мережа; AAd - алгоритм адаптації.

У четвертому розділі розроблені базові інформаційні компоненти для розширення засобів захисту системи доступу з метою використання опису складових частин системи захисту природною мовою.

Однією з важливих особливостей використання системи 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 (IS) повинна ґрунтуватися на описах предметних областей, які описують інтерпретацію даних, що використовуються у всіх фрагментах SD. Тому розглянемо основні компоненти IS, які необхідні для вирішення задач інформаційного забезпечення системи безпеки SD, що 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 компонентів системи BSD (Σ).

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 приймемо наступні умови.

Умова 2. Вимір зміни рівня абстракції можливий тільки між двома описами предметних областей, які мають не менше половини загальних базових елементів.

Умова 3. Вимір величини зміни рівня абстракції можливий тільки між двома описами предметних областей, що модифікуються послідовно.

Умова 4. Зміна величини рівня абстракції між двома послідовно розглянутими описами предметної області не може перевищувати 10% від загальної кількості базових елементів опису предметної області, що модифікуються.

Беручи до уваги, що опис предметної області являє собою словник S_C, наведені вище умови можна описати формально. Для цього приймемо, що послідовне перетворення S_C, що приводить до зміни рівня абстракції певного опису предметної області, у загальному виді запишеться наступним співвідношенням:

$$A(S_C) = \{S_{C1} \to [F_{A1}(S_{C1}) = S_{C2}] \to ... \to [F_{A(n-1)}(S_{C(n-1)})] \to S_{Cn},$$

де F_{Ai} - перетворення S_{Ci}, що приводить до збільшення рівня абстракції опису предметної області S_{Ci}. У цьому випадку умова 2 запишеться у вигляді наступного співвідношення:

$$[S_{Ci} \cap S_{C,(i+1)} = 1/2(S_{Ci} \,\&\, S_{C,(i+1)})] \to U_{Ai}[F_{Ai}(S_{Ci})],$$

де U_{Ai} - функція, що визначає величину зміни рівня абстракції в $S_{C(i+1)}$, який реалізується співвідношенням $F_{Ai}(S_{Ci}) \to S_{C,(i+1)}$.

Умова 3 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 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 використовується для обчислення $Q_{Ai}(S_{Ci})$. У найпростішому випадку, цей параметр являє собою потужність множини S_{Ci}.

Інформаційна технологія значною мірою ґрунтується на інформаційних елементах. Особливістю інформаційних елементів є їхня залежність від опису їхньої інтерпретації $T(x_i)$, де x_i - інформаційний елемент, $T(x_i)$ - опис його інтерпретації.

Базовими складовими інформаційних компонентів є речення або фрази мови, що використовується для формування $T(x_i)$. У більшості випадків, як така мова вибирається природна мова, особливо, якщо йдеться про систему за участю користувачів. Тому, важливими компонентами інформаційних засобів є синтаксис і семантика відповідної мови. В роботі розглянуті ці компоненти в рамках обмежень, які визначаються особливостями й задачами системи безпеки доступу BSD.

На рис. 6 зображена структурна схема засобів інформаційного забезпечення системи безпеки системи доступу до об'єкта доступу. На рисунку використовуються наступні позначення:

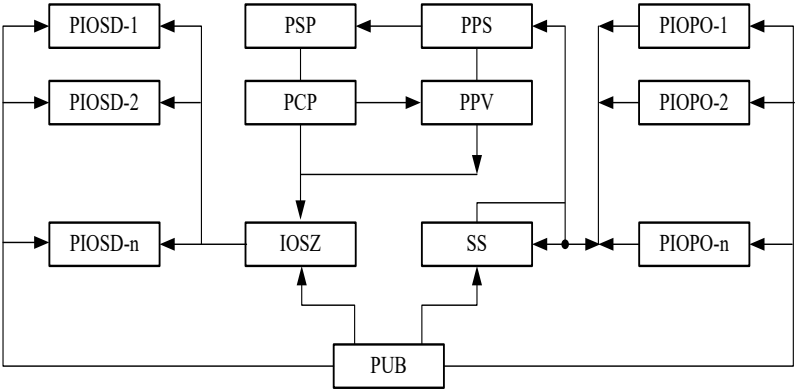


Рисунок 6 – Структурна схема засобів інформаційного забезпечення системи безпеки SD

- $PIOSD-i$ - 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 виводу;
- SS - семантичний словник;
- PUB - підсистема керування безпекою.

Підсистема $PIOSD-i$ містить опис предметної області системи доступу. Предметна область системи доступу являє собою опис всіх засобів, які використовуються або можуть використовуватися для вирішення задач безпосередньо пов'язаних з реалізацією доступу користувача до об'єкта доступу і засобів або опису предметної області, що пов'язане з вирішенням задач забезпечення безпеки системи доступу.

Природно припустити, що міра розширення засобів захисту в системі доступу впливає на величину безпеки функціонування відповідної SD. Тому розглянемо засоби, які можуть використовуватися в рамках SD, для забезпечення безпеки

функціонування системи. До таких засобів, які відповідають різним аспектам забезпечення безпеки та відображають різні підходи до забезпечення безпеки системи доступу в цілому, можна віднести наступні:

– засоби ідентифікації користувача (SIP);

– засоби автентифікації користувача на основі різних інформаційних підходів (SAI);

– засоби автентифікації на основі поділу таємної інформації (SAT);

– засоби виявлення аномалій у SD на основі використання нейронних мереж (VAN);

– виявлення аномалій у SD на основі імовірнісних моделей (VAV);

– засоби контролю доступу на основі використання різних моделей доступу (SKD) та ін.

Кожне з наведених вище засобів, по суті, являє собою окремий фрагмент предметної області системи SD розширеної до системи BSD. Очевидно, що для кожної окремої SD немає необхідності використовувати всі існуючі засоби для забезпечення безпеки SD, оскільки вимоги до рівня безпеки для різних SD можуть бути різними. У зв'язку із цим необхідно вирішити задачу визначення та розробки методів і розробки оцінки рівня безпеки, що забезпечується кожним окремим засобом.

Другою важливою задачею є задача встановлення взаємозв'язків між окремими засобами. На підставі таких взаємозв'язків можна будувати впорядковану структуру системи BSD, в яку входять окремі засоби безпеки. В межах цієї структури впорядкування може вестися стосовно величини безпеки, що забезпечує кожний із засобів.

Третьою задачею, яку необхідно вирішувати, є побудова для кожного із засобів або для кожного фрагмента відповідної області предметної інтерпретації індивідуальних інформаційних розширень, за допомогою яких можна зв'язувати між собою засоби захисту різних типів.

Черговою задачею, яку необхідно вирішувати і яка безпосередньо пов'язана з попередніми задачами, є задача формування формальних засобів опису інформаційних моделей, що дозволить здійснювати необхідні узагальнення побудованих інформаційних моделей. Таке узагальнення дозволить спростити методи вирішення задач формування структури системи захисту SD, в яку може входити цілий ряд окремих засобів захисту SD.

Необхідно в такий спосіб сформувати фрагменти семантичних словників для відповідних предметних областей, щоб виявилося можливим рішення задач захисту не тільки в рамках певної реалізації одного з варіантів алгоритму контролю доступу, але й було можливо на основі аналізу семантики відповідних описів розширювати й модифікувати відповідні алгоритми доступу. Оскільки семантичний словник S_C, в основному, являє собою опис, що використовується для відображення інтерпретаційних розширень природною мовою, то у загальному виді один елемент словника можна представити в такий спосіб:

$$x_i = < a_{i1}, a_{i2}..., a_{in} > | < a_{k1}, a_{k2}, ..., a_{km} > | ... < a_{j1}, ..., a_{jk} >,$$

де $< a_{j1}, ..., a_{jk} >$ - окремий фрагмент текстового опису інтерпретаційного розширення для x_i, a_{ij} - окреме слово відповідного фрагмента. Фрагментом $\phi_i(a_{i1}, ..., a_{in})$ може

служити фраза, речення або інша конструкція, що визначається синтаксичними схемами.

Для випадку схем сильної ідентифікації окремі елементи предметної області можуть у рамках семантичного словника описуватися в такий спосіб:

$SP =$ <санкціонований користувач>

$NP =$ <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 блокового алгоритму A_1 }

$A_m =< x_m(A_m) >\rightarrow$ { опис блокового 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 $< x_i(A_i) >$ і $< x_i(S_i) >$, являють собою скорочені описи алгоритму і схеми доступу, що використовуються тільки в рамках наведеного прикладу опису фрагмента опису S_C.

Використання семантики, у традиційних підходах, обмежується автоматизацією процесів відображення необхідної для користувача інформації при формуванні дружнього інтерфейсу. У звичайному випадку, функції семантики розглядаються значно ширше. Це розширення орієнтоване на обґрунтування можливості використання особливостей семантики об'єктів, які досліджуються для опису спеціальних семантичних параметрів, які дозволяють проводити кількісний аналіз семантичних факторів. У зв'язку із цим виникає необхідність на певному рівні семантичних описів перейти від особливостей відображення семантики до формальних оцінок відповідних особливостей.

Головними особливостями семантичних описів є наступні:

– якісний характер таких описів;

– наявність кількісної невизначеності, що відображається у відповідних описах;

– суб'єктивність уточнень або інтерпретації невизначеності описів.

Для здійснення переходу від описів семантики, які мають наведені вище особливості, до формалізованого опису характеристик семантики об'єктів, що розглядаються, необхідно прийняти наступні угоди:

– описи інтерпретаційних розширень об'єктів здійснювати у формалізованій формі;

– увести певні вихідні умови заміни текстового опису семантики прийнятими числовими величинами на шкоду можливостей розширення або розширення якісних можливостей відповідних описів.

Інтерпретаційні розширення, які використовуються для опису базових елементів системи, є основою для обчислення семантичних параметрів окремих елементів описів і фрагментів таких описів інформаційних компонентів. У зв'язку із 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 певне число елементів, що є в основному словами природної мови.

В роботі проведено дослідження взаємозв'язків між семантичними параметрами. Введено наступні семантичні параметри, які будуть характеризувати семантику інформаційних засобів системи BSD, які допускають текстове відображення природною мовою:

– семантична значимість елемента (z);

– семантична ефективність елемента (e);

– суперечливість фрагмента (h);

– погодженість фрагментів у пропозиції (u);

– рівень конфліктності пропозицій (k).

Розглянемо способи визначення їхніх числових значень, для чого розглянемо наступні визначення.

Визначення 6. Величина семантичної значимості елемента визначається числом інформаційних компонентів, які використовуються для опису інтерпретаційних розширень відповідних елементів x_i.

Визначення 7. Величина семантичної ефективності елементів x_i визначається частотою використання відповідних елементів в алгоритмах рішення прикладних задач.

Визначення 8. Суперечливість фрагментів $h(\phi_i)$ визначається функцією f семантичних параметрів слів з z і E, які використовуються для формування відповідного фрагмента.

Визначення 9. Міра непогодженості $u(\phi_1, ..., \phi_m)$ між фрагментами пропозиції Ψ визначається на основі максимальних значень величин суперечливості в кожному із фрагментів ϕ_i.

Визначення 10. Потенційна конфліктність $K(\Psi_i, \Psi_{i+1})$ між двома послідовними пропозиціями дорівнює абсолютному значенню різниці мір їхньої непогодженості.

Необхідність дослідження взаємозв'язків між семантичними параметрами обумовлюється наступними факторами й особливостями цих параметрів:

– існуванням взаємозалежностей між параметрами, які описуються в їхніх визначеннях;

– необхідністю семантичної інтерпретації різних значень величини цих параметрів;

– існуванням критичних значень величин семантичних параметрів, обмеженими діапазонами їхніх значень і особливих точок значень відповідних параметрів.

Введення чисельних значень семантичних параметрів має сенс, якщо семантичною інтерпретацією володіють не тільки самі параметри, але й окремі величини їхніх значень. Установлення такої інтерпретації можна здійснювати такими 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 й змін у текстових описах у цілому, при зміні значень окремих параметрів;

– на основі об'єктивних обмежень, які накладаються на діапазони значень параметрів, виходячи з аналізу специфіки предметної області.

Для визначення верхньої границі кількості припустимих слів у межах фрази ϕ^j введемо додатковий семантичний параметр, що описується наступним визначенням.

Визначення 11. Семантичний надлишок фрази $\eta(\phi_i)$ визначається похідною від функції $f(z_i)$, яка визначена на ϕ_i, по змінній, що співпадає з віссю розташування слів у фразі ϕ_i.

У п'ятому розділі розглянуті основні способи реалізації процесів адаптації, при вирішенні задач захисту систем доступу.

Визначення 12. Процесом адаптації в системі SD 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.

Виходячи з наведеного визначення видно, що в процесі адаптації не здійснюється структурних змін системи аналізу об'єктів.

Розглянемо ряд умов які повинні виконуватися для того, щоб могли реалізовуватися дії в SD, що класифікуються як дії процесів адаптації. Почнемо з умови, яка визначає допустимість зміни оцінки значення параметра p_i, що аналізується.

Умова 5. 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 й β граничні значення діапазону значень параметра p_i, α_i - перевищення граничного значення α або нова верхня границя, β_i - нова нижня границя β значення параметра p_i, n - кількість випадків перевищення значень параметра p_i верхнього припустимого значення.

Наведена умова ініціалізації процесу адаптації відповідає випадку модифікації граничних значень контрольованих параметрів і відноситься до випадку реалізації в SD граничних алгоритмів контролю доступу.

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 певної умови. Сформулюємо таку умову в такий спосіб.

Умова 6. Кількість m параметрів P_i у SD може бути збільшена на величину k,

якщо має місце наступне співвідношення:

$$\forall k \exists B(x_1, x_2, \cdots, x_N)\left[\left[(B \rightarrow P_{jk}) \& \left(s \rightarrow \left[s^* = f_k(s, P_{jk})\right]\right)\right]\right] \rightarrow (P_{jk} \in SD),$$

де $B(x_1, x_2, \cdots, x_N)$ - система формул, яка описує процеси визначення несанкціонованого звертання до SD, s^* - система захисту, у якій передбачається виконання аналізу P_{jk} відповідно до функції f_k. Виходячи із 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 s.

Умова 7. Кількість m параметрів P_i у SD може бути зменшена на k, якщо виконується наступне співвідношення:

$$\forall K \exists \left[u(s^*) \geq u(c) \right] \exists s(P_1, \cdots, P_N) \left[\left[s(P_1, \cdots, P_N) \rightarrow s^*(P_1, \cdots, P_{N-k}) \right] \& \, SD(s^*) \right] \rightarrow SD / \sum_{N-k}^{N} P_j,$$

де $u(s^*)$ - опис рівня безпеки, який забезпечує система SD;

$u(c)$ - опис рівня безпеки SD, який визначений як мета;

$s(P_1, \cdots, P_N)$ - система захисту, яка входить в SD і здійснює захист OD із заданим рівнем $u(c)$;

$s^*(P_1, \cdots, P_{N-K})$ - логічна система аналізу безпеки доступу, яка може бути виведена з $s(P_1, \cdots, P_N)$.

Далі в роботі проаналізовано ще й наступні аспекти, які є загальними для системи, що володіє властивостями адаптації: визначено цілі процесів адаптації; визначено тривалість процесів адаптації; визначено можливості методів адаптації в вирішенні задач SD забезпечення безпеки при факторах, що змінюються, які ініціюють або пов'язані із процесами адаптації.

Цілі процесів адаптації можна розділити на: локальні цілі; інтегральна ціль; умовні або виділені цілі.

Процеси адаптації, які приводять 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; сполучений спосіб реалізації процесів адаптації.

У найпростішому випадку під узагальненим процесом адаптації можна мати на увазі суму всіх процесів адаптації, що відбуваються в мережі, яка 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, у яких протягом інтервалу ΔT_i відбулися процеси адаптації $A_i(S)$, n - загальна кількість фрагментів у мережі S.

У межах 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 SD системи.

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 у порівнянні з використанням простих критеріїв. У рамках теорії перспектив, процес ухвалення рішення, фактично складається із двох компонентів - компоненти придбання досвіду і компоненти безпосереднього ухвалення рішення. Відповідно до теорії перспектив приймається, що оцінюється кожний вибір і здійснюється вибір того варіанта, що має найбільшу вагу. Така вага визначається двома ваговими функціями $\pi(p)$ й $v(x)$, де $\pi(p)$ пов'язане з ймовірністю p, а $v(x)$ відображає суб'єктивну вартість вибору x. Формально, така функція вибору описується співвідношенням:

$$V(x, p, y, q) = \pi(p)\, v(x) + \pi(y)\, v(y).$$

У межах цього підходу, заміна ймовірності p ваговою функцією $\pi(p)$ являє собою узагальнення традиційної концепції корисності.

У теорії корисності та теорії перспектив вирішується задача, що описує, як реалізується процес ухвалення рішення. При цьому, не менш важливими є нормативні проблеми, які полягають у тому, щоб визначити чисельні способи визначення вагових функцій $\pi(p)$ і $v(x)$.

Для оцінки очікуваних втрат і небезпек можна розглянути двофакторну функцію марності, що 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 засоби, що забезпечують позитивний результат модифікації пов'язаної з адаптаційними змінами у фрагментах нейронної мережі, R_γ - очікувана одиниця втрат з моделлю двофакторного розкладання $R_{lu} = 1 - (K_l^* / K_l) > 0$ з імовірністю P_l і $R_{ld} = 0$ з імовірністю $1 - P_l$, K_l - величина, що 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 від'ємній величині 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 границя втрат або $P_l \le P_l^*$. Приймемо, що функція $D_i(X_{li})$ опукла або $\beta_l > 1$. Тоді функція марності 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, що характеризує мотивацію прийняття рішень. Це можна здійснити аналогічно способу визначення коефіцієнта β для функції корисності. У цьому випадку, розглядається параметр C, що визначає величину компенсації втрат, при виникненні ситуації, при якій мало місце успішне несанкціоноване втручання.

У межах розглянутого підходу, фрагмент нейронної мережі, що використовується для формування всієї мережі, відрізняється рядом особливостей від фрагментів традиційних мереж. Ці особливості полягають у наступному:

– класичний суматор, що є базовим елементом нейрона, має додаткові функціональні входи;

– крім суматора і вузла, який 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 рисою окремого нейрона і нейронної мережі, у цілому, є простота реалізації окремих елементів мережі, розглянемо способи реалізації додаткових компонентів 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, відповідно до реалізованого алгоритму, 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, що поступають з виходу функціонального блоку аналізу вхідних змінних, котрий у класичному випадку являє собою суматор 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 із блоку аналізу критеріїв адаптації та сигналів, які формуються на виході блоку суматора нейрона. Формально, ефект адаптації на $i-$ому процесі адаптації для $j-$го 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 $j-$го BS, котрий синхронізується ініціалізацією процесу адаптації суматора BS_i, що 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 наведена на рис. 7.

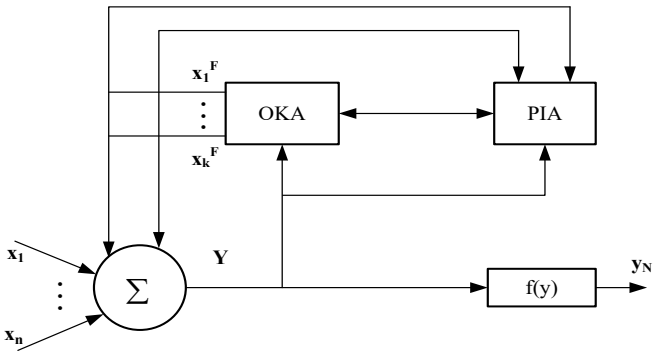


Рисунок 7 – Функціональна схема модифікованого елемента нейронної мережі

де: $\sum$ – блок підсумовування вхідних параметрів або вхідний 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.

У випадку використання критерію $V(x,p_i,y,q)$, параметрами є ймовірності p_i та q, а також події x_i та y_i – які відображають значення на виході у випадку коли враховується можливий ризик, що пов'язаний з функціонуванням нейрона. При цьому ймовірності різних виходів замінюються функціями, які, по суті, повинні їх інтерполювати. Такі функції формуються виходячи з даних історії з факторів обумовлених змінами функції перспективи $V(x,p_i,y,q)$.

У шостому розділі описана апробація методів та моделей розмежування доступу до інформаційних ресурсів.

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.

На рис. 8 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.

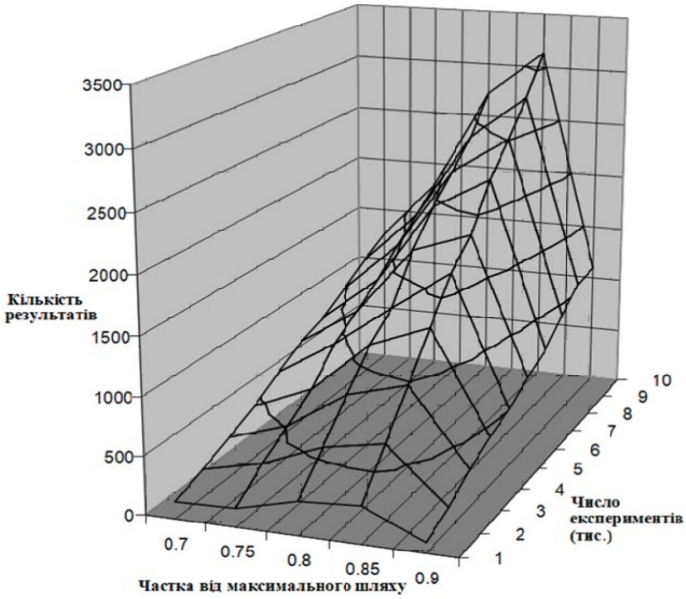


Рисунок 8 – Скорочення шляху при рівномірному розподілі

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 (див. рис. 9) та за рукописним почерком відповідно. Для формування та динамічного передавання характеристик почерку користувача в комп'ютер в даних системах використовуються клавіатура та графічний планшет відповідно. Необхідною складовою частиною даних систем автентифікації є первинна обробка зразків почерку, відповідна до біометричного методу, який використовувався. В даних системах досить суттєвий вплив на імовірність

правильного розпізнавання користувачів мають: правильний вибір фрази (слова), динаміка вводу і стиль та правильність написання якої аналізується відповідно; налаштування параметрів, які є найбільш критичними при роботі даних систем автентифікації користувачів за обраними біометричними характеристиками. В обох системах в якості механізму розпізнавання використовується імовірнісна нейронна мережа.

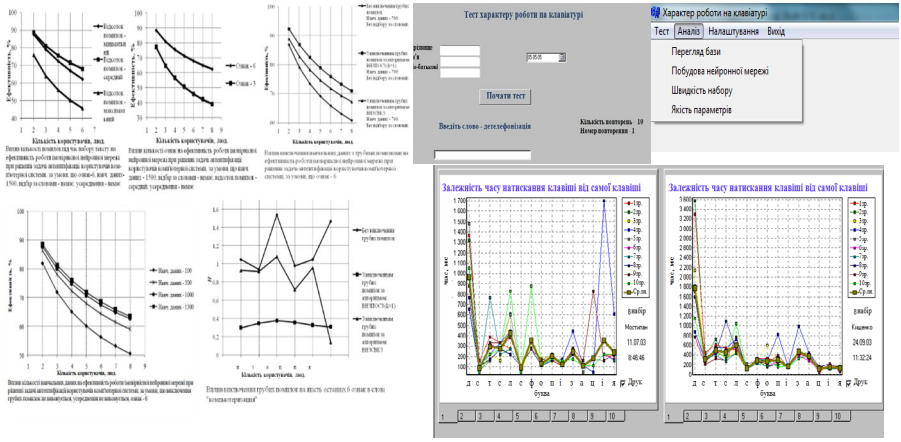


Рисунок 9 – Система автентифікації користувачів за їх клавіатурним почерком

Невід'ємною складовою застосування будь-якої комплексної системи захисту інформації є проведення її експертизи. Відповідно було розроблено програмний застосунок методу ідентифікації функціонального профілю захисту системи підтримки прийняття рішень при проведенні експертиз КСЗІ (див. рис. 10). Реалізація даного застосунка призначена для допомоги експерту при визначенні функціонального профілю захисту в документі Microsoft Word, а також допомагає експерту при аналізі даного профілю. Головною метою цього програмного застосунка є допомога експерту при створенні функціонального профілю захисту 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 функціональними профілями захисту молодших; перевірка взаємопов'язаності функціональних послуг безпеки.

Результати дисертаційної роботи застосовувалися при проведенні наступних практичних робіт з експертизи технічних систем захисту: експертиза «Комутатор зв'язку КС ТУ У 31016953.001-2000»; державні експертизи комплексних систем захисту інформації: українського академічного грід-вузла Інституту теоретичної фізики НАН України, Центру реєстрації віртуальних організацій, в автоматизованій системі управління персоналом "Кадри" рівня Укрзалізниці, автоматизованої інформаційної системи Президії Національної академії наук України, локальної обчислювальної мережі Управління справами НАН України, Національного Ресурсного центру Інституту кібернетики НАН України ім. В.М. Глушкова, на об'єкті, що належить 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.

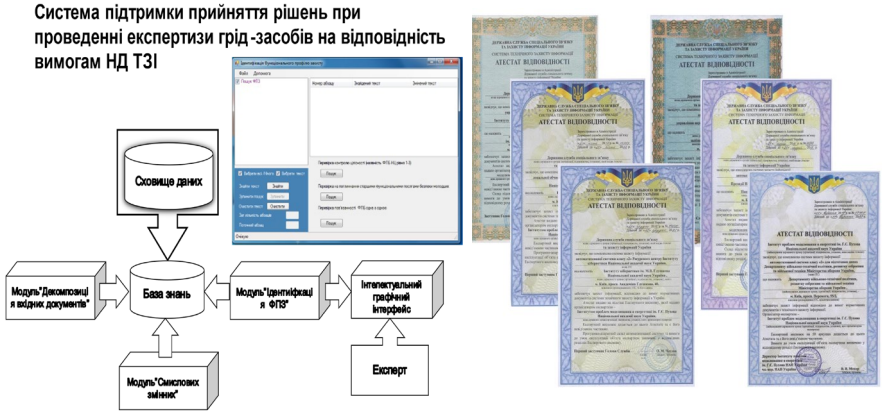


Рисунок 10 – Програмний застосунок методу ідентифікації функціонального профілю захисту системи підтримки прийняття рішень при проведенні експертиз КСЗІ

Також було 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.

Даний грід-сервіс повинен задовольняти наступним вимогам:

– 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.

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.

Відповідно до проведеного аналізу та вибору підходів для забезпечення необхідних функцій віддаленого синтезу конфігурацій ПЛІС було запропоновано наступну архітектуру грід-сервісу (див. рис. 11).

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.

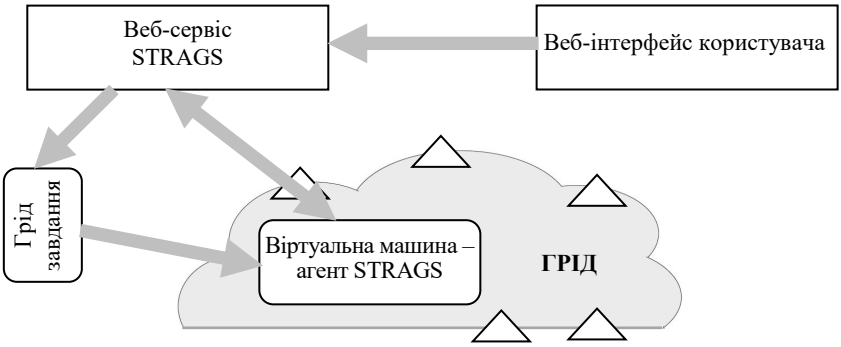


Рисунок 11 – Компоненти грід-сервісу STRAGS

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.

У додатках містяться документи, що підтверджують впровадження результатів дисертаційної роботи, та лістинг розроблених програмних застосунків безпеки систем розмежування доступу та інших розробок.

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.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

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.

АНОТАЦІЯ

Давиденко А.М. Методи та моделі адаптивного захисту та розмежування доступу до розподілених інформаційних ресурсів. – Рукопис.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації». – Національний авіаційний університет. Київ, 2021.

Дисертація присвячена питанням створення методу адаптації систем розмежування доступу до розподілених інформаційних ресурсів, що реалізує налаштування засобів захисту системи розмежування доступу до поточного стану безпеки на основі використання параметрів процесу обробки інформації, що дозволило зменшити втрати часу за рахунок узгодження процесів оброки інформації та надання доступу до неї. Розроблено розширену математичну модель елемента нейронної мережі для вирішення задач адаптації, обґрунтована доцільність її використання в системі розмежування доступу, висвітлені проблеми, що виникають при цьому, й шляхи їх подолання. Досліджено методи організації контролю даних, які використовуються для ідентифікації в системах доступу. Розроблено методи самоорганізації засобів доступу, що дозволило автоматизувати модифікацію елементів системи захисту в ході реалізації процесу адаптації. Запропоновано базові інформаційні компоненти, що розширяють засоби захисту системи доступу, завдяки чому стало можливим узгоджувати швидкодію процесів оброці інформації та надання доступу до ней, шляхом налаштування відповідних параметрів, що дозволило розширити предметну область за рахунок адаптації контролю доступу. Запропоновано метод адаптації системи розмежування доступу до інформації, при якому система здатна підлаштовуватися до реально існуючих загроз і атак, змінюючи рівень захищеності, а відтак змінюючи й кількість використовуваних для його реалізації ресурсів, що напряму знижує навантаження з боку системи захисту на загальну продуктивність системи. На основі теоретичних досліджень реалізовані засоби захисту для ідентифікації за клавіатурним почерком з адаптацією до його змін. Розроблено й випробувано методи загальної організації використання запропонованої технології при проектуванні конкретних адаптивних систем захисту доступу до інформаційних ресурсів.

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. – Manuscript.

Thesis for a Doctor of Technical Sciences degree in the specialty 05.13.21 - «Information Security Systems». - National Aviation University. Kyiv, 2021.

The dissertation work solves and investigates the scientific and technical problem, which consists in solving the contradiction between the need for high-performance processing of information resources with limited access, the parallel processing of which puts forward high requirements for the speed of their preparation and single-threaded mechanisms for differentiation of access cannot provide them, so it is proposed to develop methods and models that can coordinate the performance of

processing and protection methods and adapt them to each other for high-performance and safe existence in distributed information , which allows to obtain new solutions for scientific and technical problems of the formation of a system of differentiation of access to information resources of a person, society and the state on the basis of the use of protection models, which by means of prompt adjustment of the process of control of access separation, including on the basis of neural networks, allowed to give the appropriate subsystem of protection properties of adaptation in relation to the criteria determined by the parameters of the system security level and parameters that characterize the processes of information processing in specialized distributed information systems.

An important problem that needs to be solved when designing protections for the access system is the implementation of such protections that could independently adapt to certain changes that occur at the needs of users of the relevant system. In this case, there are problems of recognition of authorized or legal users, the task of adapting the parameters of the means of protection and the protection system as a whole to external changes that occur in users. On the other hand, taking into account that the means of protection, depending on the level of protection they provide, have different costs and consume different amounts of computer network resources, and taking into account other factors, it may turn out that this or that information over time changes the required level of its protection. In this case, it is advisable to design access system protection in this way so that automatically, regardless of the network administrator, the level of protection that these tools provide could change. From the above it follows that the means of protection, which are inherent in the above properties, should be built on the basis of a theoretical apparatus and such tools that would ensure the implementation of the necessary algorithms for solving these problems to the maximum extent possible. One of these tools, which could to the greatest extent provide the possibility of solving these problems, are neural networks.

The dissertation is devoted to the issues of creating a method for the functioning of information security systems, which implements the settings of the means of protecting the system of access to information resources to the current degree of danger based on the use of parameters of the information processing process, which made it possible to reduce the loss of time by coordinating information processing processes and providing access to it. An extended mathematical model of an element of a neural network for solving adaptation problems has been developed, the expediency of its use has been substantiated, investigated that allow adjusting the parameters of a neural network that controls the access system adequately to the real position of objects, the problems that arise in this case, and ways to overcome them are highlighted. Methods of organizing data control, which are used for identification in access systems, have been investigated. Methods of self-organization of access means have been developed, which made it possible to automate the modification of the elements of the protection system during the implementation of the adaptation process. Basic information components are proposed that expand the security means of the access system, due to which it became possible to coordinate the speed of information processing and provision of access to it by setting the appropriate parameters, which made it possible to expand the subject area by adapting access control. A method for the functioning of the information security system is proposed, in which the system is able to quickly adapt to real-life threats and attacks, changing the level of security, and accordingly changing the number of resources used for its implementation, which directly

determines the cost of functioning of the security system. On the basis of theoretical research, security tools for identification by keyboard handwriting with adaptation to its changes have been implemented. Methods for the general organization of the use of the proposed technology in the design of specific adaptive systems for protecting access to information resources have been developed and tested.

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