**Мартовицький Віталій Олександрович, старший викла&shy;дач Харківського національного університету радіоелектро&shy;ніки: &laquo;Моделі та метод виявлення аномалій функціонування комп&rsquo;ютерних систем на основі технології машинного на&shy;вчання&raquo; (05.13.05 - комп&rsquo;ютерні системи та компоненти). Спецрада Д 64.050.14 у Національному технічному універ&shy;ситеті &laquo;Харківський політехнічний інститут&raquo;**

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ «ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова праця на правах рукопису

МАРТОВИЦЬКОГО ВІТАЛІЯ ОЛЕКСАНДРОВИЧА

УДК 004.056.53

**ДИСЕРТАЦІЯ**

**МОДЕЛІ ТА МЕТОД ВИЯВЛЕННЯ АНОМАЛІЙ ФУНКЦІОНУВАННЯ КОМП’ЮТЕРНИХ СИСТЕМ НА ОСНОВІ ТЕХНОЛОГІЇ**

**МАШИННОГО НАВЧАННЯ**

05.13.05 – комп’ютерні системи та компоненти 12 – Інформаційні технології

Подається на здобуття наукового ступеня кандидата наук

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

В.О. Мартовицький

Науковий керівник

Рубан Ігор Вікторович, доктор технічних наук, професор

Харків –2019

ЗМІСТ

[ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 5](#_bookmark0)

[ВСТУП 7](#_bookmark1)

1. [Аналіз сучасного стану підходів виявлення аномалій в комп’ютерних системах 19](#_bookmark2)
   1. [Аналіз принципів функціонування комп’ютерних систем 19](#_bookmark3)
      1. [Аналіз особливостей функціонування розподілених комп’ютерних систем 26](#_bookmark4)
      2. [Аналіз підходів щодо забезпечення безпеки розподілених комп’ютерних систем 34](#_bookmark5)
   2. [Аналіз принципів побудови сучасних систем моніторингу розподілених комп’ютерних систем 37](#_bookmark6)
   3. [Аналіз сучасних методів виявлення атак 44](#_bookmark7)
      1. [Критерії порівняння методів виявлення атак 44](#_bookmark8)
      2. [Аналіз методів виявлення аномалій 49](#_bookmark9)
   4. [Вибір методів оцінки результатів роботи програмних додатків виявлення аномалій 59](#_bookmark10)

[Висновки до розділу 1 64](#_bookmark11)

1. [РОЗРОБКА МОДЕЛІ МОНІТОРИНГУ АНОМАЛІЙ 66](#_bookmark12)
   1. [Архітектура та модель функціонування розподілених комп’ютерних систем 66](#_bookmark13)
      1. [Архітектура розподілених комп’ютерних системи 66](#_bookmark14)
      2. [Модель функціонування розподілених комп’ютерних систем на основі клієнт-серверної архітектури 75](#_bookmark15)
      3. [Формування параметрів моніторингу інфраструктури і застосувань в розподілених комп’ютерних системах 82](#_bookmark16)
   2. [Структура моделі моніторингу аномалій 90](#_bookmark17)
   3. [Мультиагентна підсистеми збору та зберігання даних 99](#_bookmark18)
      1. [Структура мультиагентної підсистеми збору та зберігання даних 101](#_bookmark19)
      2. [Модель мультиагентної підсистеми збору та зберігання даних](#_bookmark20)

[........................................................................................................................... 105](#_bookmark20)

* + 1. [Протокол взаємодії агентів моніторингу в розподілених компютерних системах 108](#_bookmark21)

[Висновки до розділу 2 112](#_bookmark22)

1. [РОЗРОБКА МЕТОДУ КЛАСИФІКАЦІЇ АНОМАЛІЙ 114](#_bookmark23)
   1. [Формулювання підходів щодо вирішення завдань класифікації аномалій 114](#_bookmark24)
      1. [Дослідження принципів послідовно навчання базових алгоритмів 116](#_bookmark25)
      2. [Дослідження принципів комбінації алгоритмів методом голосування по більшості 119](#_bookmark26)
      3. [Дослідження принципів комбінації алгоритмів методом голосування по старшинству 122](#_bookmark27)
      4. [Дослідження принципів комбінації алгоритмів методом Boosting 124](#_bookmark28)
      5. [Дослідження принципів комбінації алгоритмів методом bagging і методом випадкових підпросторів 129](#_bookmark29)
      6. [Дослідження принципів комбінації алгоритмів методом stacking](#_bookmark30)

[........................................................................................................................... 132](#_bookmark30)

* 1. [Метод до класифікації стану мережі на основі статистичних параметрів для виявлення аномалії в інформаційній структурі обчислювальної системи 134](#_bookmark31)
     1. [Постановка задачі класифікації стану мережі 136](#_bookmark32)
     2. [Метод класифікації стану мережі на основі модифікованого алгоритму стекинга 139](#_bookmark33)
     3. [Результати дослідження методів класифікації стану мережі 142](#_bookmark34)
  2. [Відбір параметрів моніторингу мережної інфраструктури для класифікації стану мережі 146](#_bookmark35)

[Висновки до розділу 3 157](#_bookmark36)

1. [РОЗРОБКА ТЕХНОЛОГІЇ МОНІТОРИНГУ СТАНУ ФУНКЦІОНУВАННЯ РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМИ 158](#_bookmark37)
   1. [Розробка методики моніторингу стану функціонування розподілених компютерних системи 158](#_bookmark38)
   2. [Архітектура мультиагентної системи моніторингу 161](#_bookmark39)
   3. [Розробка автоматизованого робочого місця адміністратора сервера моніторингу 167](#_bookmark40)

[Висновки до розділу 4 175](#_bookmark41)

[ВИСНОВКИ 176](#_bookmark42)

[Список використаних джерел 178](#_bookmark43)

[ДОДАТОК А 190](#_bookmark44)

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

БД – база даних

ПЗ – програмне забезпечення ОС – операційна система

JSON – JavaScript Object Notation XML – eXtensible Markup Language MIB – Management Information Base

SNMP – Simple Network Management Protocol ІС – інформаційна система

РС– розподілена система

РКС– розподілена комп’ютерно система IDL – Interface Definition Language

ЕОМ – електронна обчислювальна машина СБІ – системи безпеки інформації

СВВ – система виявлення вторгнень

HIDS – Host-based Intrusion Detection System NIDS – Network Intrusion Detection System АIDS – Аpplication Intrusion Detection System SVM – support vector machine

I/O – input/output

ЛОМ – локальна обчислювальна мережа МАС – мультиагентна система

AMS - Agent Management System DF – Directory Facilitator

PDM – Protocol Data Messages USE – utilization, saturation, errors OOM – Out of memory

SLA – service level agreements AID – Agent identificator

OSI – sytems interconnection basic reference model

ВСТУП

**Актуальність** теми дослідження полягає у тому, що сучасний рівень розвитку інформаційної техніки і технологій дозволяє створювати пристрої та системи різного призначення і масштабу для широкого спектра задач моніторингу. Моніторинг просторово розподілених параметрів передбачає істотне використання мережних технологій, де останнім часом також спостерігається вражаючий прогрес. Цей прогрес характеризується наступними головними тенденціями: спеціалізація мереж, зміна характеру мережних додатків і спільне використання мереж різних типів.

Розуміння стану інфраструктури та систем важливо для стабільної роботи сервісів. Інформація про працездатність і продуктивності розгортання не тільки допомагає команді вчасно реагувати на проблеми, але і дає їм можливість впевнено вносити всі необхідні зміни. Один з кращих способів отримати цю інформацію є надійна система моніторингу, яка збирає метрики системи, візуалізує дані і попереджає операторів, про кібернетичні впливи на комп’ютерну систему.

У системах моніторингу мережної інфраструктури відбуваються радикальні зміни, викликані загостренням конкуренції на ринку, зростанням вимог до якості забезпечення безпеки, технічним переозброєнням мереж зв'язку, зміною характеру розподілу трафіка. Все це призводить до необхідності здійснення контролю великої кількості параметрів функціонування мереж різних технологій.

Система моніторингу не тільки змінює уявлення про систему експлуатації, переходячи від збору даних параметрів окремих станцій до параметрів експлуатації всієї мережі, а також автоматизує безліч рутинних процесів зі збору та обробки параметрів розподіленої комп’ютерної системи.

Аналіз цієї інформації дає можливість виявлення різноманітних випадків загроз та порушень, таких як:

* несанкціоноване підключення до мережі, пропущене класичними засобами захисту периметра (IPS / IDS);
* поширення вірусів і шпигунського програмного забезпечення, не виявлених штатними антивірусними засобами;
* неправильні дії при користуванні ресурсами розподілених комп’ютерних систем. Наприклад, масштабні завантаження з торрент- трекерів, звернення до сегментів мережі, до яких немає доступу, спроба доступу до конфіденційної інформації та інше;
* підключення в мережу нових пристроїв і їх поведінка;
* помилки в роботі обладнання;
* виникнення в мережі «вузьких» місць і інші можливі порушення. Архітектура системи моніторингу параметрів отриманих від датчиків,

характеризуються не тільки їх цільовими функціями, але і функціональними можливостями, що забезпечують реалізацію цільових функцій, ієрархією та рівнем паралелізму вирішення завдань, однорідністю або різнорідністю модульної структури, організацією збору інформації в режимі реального часу, обробки даних і мережного обміну інформацією з абонентами.

При цьому повинні забезпечуватися:

* невтручання в роботу мережного обладнання;
* постійний збір статистичної інформації, який дозволяє створювати повномасштабні бази даних, необхідні для проведення аналізу параметрів мережі в масштабі реального часу;
* забезпечення високої швидкості обробки запитів на надання потрібних інформаційних ресурсів і сервісів;
* виконання збору, обробки, зберігання повної інформації про стан всіх компонентів телекомунікаційної і інформаційної інфраструктури мережі в реальному часі незалежно від архітектури мережі, типу комутатора і постачальника;
* створення єдиного стандартизованого інформаційного центру зберігання даних про стан систем і мережі.

З огляду на великий обсяг подій, що супроводжують процес діагностичного моніторингу, різноманіття типів подій і пристроїв у відкритій системі, що діагностується, і необхідність функціонування в режимі реального часу з урахуванням високої мінливості зовнішнього середовища, завдання побудови діагностичного моніторингу мережі слід віднести до проблематики обробки великих даних. Рішення даної проблеми пов'язане з реалізацією нових парадигм розробки програмних систем, підтримуючих можливість розподіленої взаємодії автономних активних пристроїв в процесі вирішення конкретного оперативного завдання.

**Об'єктом дослідження** є процес моніторингу стану інформаційного та комунікаційного середовища розподілених комп’ютерних систем.

**Предметом дослідження** є методи і алгоритми моніторингу в розподілених комп’ютерних системах із застосуванням технологій інтелектуального аналізу даних.

**Метою дисертаційної роботи** є покращення показників виявлення аномалій функціонування РКС в умовах кібернетичних впливів зовнішнього та внутрішнього середовища шляхом побудови моделей і методів на основі технологій інтелектуального аналізу даних.

Для досягнення поставленої мети вирішуються наступні задачі:

* проаналізувати підходи щодо забезпечення безпеки розподілених комп’ютерних систем;
* розглянути особливості архітектури розподілених комп’ютерних систем і виділити базові компоненти систем;
* визначити множину параметрів для оцінки кожного елемента системи;
* розробити метод виявлення аномалій системи з використанням методів інтелектуального аналізу для класифікації стану функціонування комп’ютерних систем;
* розробити структуру мультиагентної системи моніторингу стану розподілених комп’ютерних систем;
* розробити методику моніторингу стану функціонування комп’ютерних систем;
* провести апробацію моделі та методів при вирішенні практичних завдань.

**Наукова новизна отриманих результатів.** Основні результати, які визначають наукову новизну дисертаційної роботи, полягають у такому:

* вперше запропонована модель класифікації стану системи, яка ґрунтується на структурному представлені показників функціональності розподілених комп’ютерних систем, що дозволяє виділити множину станів в залежності від функціональних завдань, розмежувати процеси цільового функціонування системи та інтерфейсні процеси взаємодії з мережною інфраструктурою та використовувати їх в методах інтелектуального аналізу для виявлення аномалій функціонування розподілених комп’ютерних систем.
* набула подальшого розвитку мультиагентна модель системи збору і зберігання інформації, що побудована на основі агентів, метою яких є надання користувачеві або інформаційній системі більш високого рівня інформації про стан мережної інфраструктури, отриманої в результаті збору та інтелектуальної обробки параметрів, що дозволило зменшити навантаження на мережу за рахунок застосування запропонованого протоколу обміну інформацією між агентами.
* удосконалено метод класифікації стану мережі на основі статистичних параметрів за рахунок рівномірної вибірки об'єктів з поверненням для формування навчальних вибірок, що дозволяє адаптувати процес навчання ансамбля класифікаторів до розмірів навчальної вибірки.

**Особистий внесок здобувача.** Всі наукові результати дисертаційної роботи, що виносяться на захист, отримані автором самостійно. У роботах, опублікованих спільно, автору належать такі результати: у роботі [1] розглянуто і проаналізовані найбільш поширені групи методів виявлення

аномалій. Показано, що методи виявлення атак в сучасних системах виявлення атак недостатньо опрацьовані в частині формальної моделі атаки, а отже, для них досить складно суворо оцінити такі властивості як обчислювальна складність, коректність, завершимість. В статті [2] проведено дослідження концепції побудови існуючих систем моніторингу кластерних суперкомп'ютерів. Встановлено недоліки в системах моніторингу, що призводять не тільки до зниження ефективності обчислювальних кластерів, а й до порушення їх безпеки. Описана формальна модель виявлення аномалій у функціонуванні обчислювального кластера. В роботі [3] досліджено підхід до класифікації стану мережі на основі статистичних параметрів. Встановлено недоліки в методах класифікації стану мережі. Розглянута базова реалізація комітету класифікаторів. Запропоновано модифікацію комітету класифікаторів з використання нейронної мережі як мета класифікатора. Проведено експеримент для класифікації стану мережі. В статті [4] розглянуто модель мультиагентної системи збору і зберігання інформації. Метою цієї системи є надання користувачеві або інформаційній системі більш високого рівня інформації про стан мережної інфраструктури, отриманої в результаті збору та інтелектуальної обробки параметрів. В роботі

1. проаналізовані різні техніки попередньої обробки та оцінки інформативності ознак при визначенні параметрів контролю мережної інфраструктури для більш ефективного інтелектуального аналізу стану мережної інфраструктури. Досліджені результати застосування методів відбору ознак для спрощення різних моделей машинного навчання. Сформовано мінімальний набір параметрів, які потрібні для моніторингу стану мережної інфраструктури. В статті [6] розглянута архітектура системи безпеки користувача, яка побудована на основі класів Membership API і Roles API. Дана реалізація користувача провайдера для управління безпекою Web- сервісів і додатків дозволяє: зберігати інформацію профілю в джерелі даних, відмінному від SQL Server, такому як XMLфайли; можливість розміщення простих Web-сервісів і додатків на базі ASP.NET на інших платформах

відмінних від Windows; коли треба реалізувати додаткову логіку при збереженні або витяганні даних профілю. Наприклад, можна застосувати перевірку достовірності, хешування, протоколювання, шифрування і стискування. В роботі [7] проведено огляд сучасних засобів виявлення вразливосте в комунікаційних мережах розподілених систем. В роботі [8] проаналізовано можливості виявлення загроз різними підсистемами і сформульовані критерії контрольованих параметрів, що дозволяють підвищити ймовірність виявлення, в тому числі, в умовах як пасивної так активної протидії порушника засобами виявлення. Сформульовані критерії можна використовувати при структурному синтезі системи безпеки або розробці пристроїв виявлення. В роботі [9] розглянута структура системи збору та зберігання інформації про параметри системи, що контролюється. В роботі [10] представлений метод класифікації стані комунікаційної мережі, який побудований на ансамблі методів машинного навчання. В роботі [11] представлена архітектура системи моніторингу мережної інфраструктури, яка дозволяє контролювати як параметри окремих компонентів так і параметри системи в цілому. В роботі [12] представлено підхід до виявлення шкідливого програмного коду з використанням методів машинного навчання. В роботі [13] представлено аналіз методів відбору інформативних ознак для контролю мережної інфраструктури розподілених комп’ютерних систем.

**Апробація результатів дисертації.** Основні положення дисертаційної роботи доповідалися на таких міжнародних конференціях і форумах:

* + 23-й Міжнародній науковій інтернет-конференції " Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення" (Тернопіль, 2017);
  + 2-й Міжнародній науково-практичній конференції "Інформаційна безпека та комп’ютерні технології" (Кропивницький: ЦНТУ, 2017);
  + 5-й, 6-й Міжнародній науково-технічній конференції «Проблеми інформатизації» (Черкаси – Баку – Бельсько-Бяла – Полтава 2017 р., Черкаси
* Баку – Бельсько-Бяла – Полтава 2018 р.);
  + 2-й Міжнародній науково-технічній конференції «Комп’ютерні та інформаційні системи і технології» (Харків: ХНУРЕ. 2018);
  + IEEE 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET) (Lviv - Slavske, Ukraine 2018)

**Структура дисертації.** Дисертаційна робота складається зі вступу, чотирьох розділів основної частини, висновків, списку використаних джерел, додатків.

У ***першому розділі*** на базі вивчення літературних джерел проведено аналіз сучасного стану підходів виявлення аномалій в комп’ютерних системах. Розглянуто особливості принципів побудови сучасних систем моніторингу розподілених комп’ютерних систем. Проаналізовано методи виявлення атак в сучасних системах виявлення атак, які недостатньо опрацьовані в частині формальної моделі атаки, а отже, для них досить складно суворо оцінити такі властивості як обчислювальна складність, коректність, закінченість та інші властивості.

У ***другому розділі*** досліджена архітектура та модель функціонування розподілених комп’ютерних систем. У ході експлуатації РКС та їх програмного забезпечення необхідно здійснювати постійний моніторинг та оцінювання статистичних характеристик використання компонентів системи, як комплексно, так і за кожною окремою підсистемою РКС, зокрема:

* + завантаженість процесора: загальна, окремою програмою, користувачами, простою процесора при очікуванні надходження нових даних тощо;
  + використання пам’яті: кеш-пам’яті, буферів пам’яті, віртуальної пам’яті, розподіленої пам’яті тощо;
  + проходження вхідного та вихідного мережного трафіку переданого різними мережними інтерфейсами по різних протоколах;
  + характеристики спеціалізованих обчислювальних пристроїв, наприклад, при використанні GPU.

Сформовано параметри моніторингу інфраструктури і додатків в розподілених комп’ютерних системах та представлена структура моделі моніторингу для виявлення аномальних подій, що дозволяє забезпечити виявлення аномалій функціонування РКС в умовах кібернетичних впливів зовнішнього та внутрішнього середовища шляхом побудови моделей і методів вирішення даного завдання на основі технологій інтелектуального аналізу даних. Розроблена модель дозволяє здійснити моніторинг РКС не тільки як єдиної обчислювальної системи, а й усіх його компонентів окремо, що дає можливість всебічно оцінити стан системи в цілому.

Виходячи з моделей моніторингу розглянутих в статтях [2,14] з технічних та інших причин логічно пов'язані дані зберігаються в різних форматах під управлінням різних систем зберігання і обробки даних. Очевидно, що для вивчення і аналізу інформації потрібно відкритий доступ до локальних і віддалених інформаційних джерел. З іншого боку, постає проблема інтеграції даних. Різні колекції параметрів стану компонентів мережі, навіть розташовані на одному фізичному вузлі, часто мають різні логічні входи і не надають можливості наскрізного зв'язування даних з різних джерел. Необхідність обліку всієї наявної інформації з певного питання вимагає від підсистеми збору і зберігання даних забезпечення прозорих для користувачів засобів доступу до розподіленої інформації.

У зв'язку з цим пропонується модель системи збору і зберігання даних, що забезпечує роботу з множиною різнорідних джерел, шляхом їх інтегрування з метою отримання більш повного збору інформації, що зв’язана. Система заснована на мультиагентному підході дозволяє не припиняти обробку запитів при виконанні модифікацій набору і структур, які використовуються в базах даних.

У ***третьому розділі*** наведено метод до класифікації стану мережі на основі статистичних параметрів для виявлення аномалії в інформаційній структурі комп’ютерної системи. Проведена оцінка ефективності запропонованого алгоритму з роботою базових класифікаторів і класичного

стекінга. Для проведення порівняльного аналізу використовувалися дані з чемпіонату по машинному навчанню KDD 2009 і дані отримані при моніторингу мережної інфраструктури учбового дата-центра розгорнутого на основі мережної файлової системи Lustre.

Збільшення кількості інформації, що обробляється комп’ютерними системами, а також економія на кількості обслуговуючого персоналу потребують використання ефективних засобів моніторингу обчислювальних ресурсів. Результатом цього є зростання кількості параметрів, які повинна відстежувати така система моніторингу. За рахунок великих потоків даних від різних датчиків зростає ймовірність пропуску адміністратором системи негативних змін в контрольованих параметрах мережі комп’ютерної системи. Для вирішення даної проблеми в системи моніторингу глобально починають впроваджувати засоби автоматизованого експертного аналізу даних, заснованого на машинному навчанні.

В розділі проведено оцінку інформативності параметрів контролю мережної інфраструктури для більш ефективного інтелектуального аналізу. Використовуючи лише ті ознаки, які мали максимальну важливість побудований простий алгоритм, середня помилка якого по метриці MSE мало чим відрізняється від XGBClassifier, але швидкість роботи алгоритму збільшилась.

У ***четвертому розділі*** для оцінки стану РКС за допомогою розробленої мультиагентної системи моніторингу була розроблена методика моніторингу.

Дана методика визначає умови і порядок оцінки стану РКС за допомогою розробленої мультиагентної системи моніторингу. Оцінка стану РКС за даною методикою є аналіз відомостей про стан РКС для виявлення подій, що не відповідають нормальному функціонуванню РКС – кібернетичним впливам.

Розроблена архітектура системи моніторингу з використанням автономних програмних агентів. Архітектура передбачає динамічне

формування ієрархічної структури, вузлом якої може виступати будь-яка сутність, що визначається джерелом даних або сенсором. Таким чином, стосовно моніторингу РКС можуть існувати метрики грід, кластерів, обчислювальних вузлів і завдань.

Для взаємодії між усіма агентами пропонується використовувати групу інтелектуальних агентів запиту метою яких є координація агентів збору інформації, реструктуризація отриманої інформації і реалізація протоколів і механізмів передачі повідомлень між усіма агентами моделі.

**Зв’язок роботи з науковими програмами, планами, темами.** Дисертаційна робота виконувалася відповідно до плану науково-технічних робіт Харківського національного університету радіоелектроніки в рамках держбюджетних тем:

* + «Створення науково-методичних основ забезпечення живучості мережевих систем обміну інформацією в умовах зовнішнього впливу потужного НВЧ випромінювання», Звіт про науководослідну роботу за договором від 20.09.2017 р. № Ф76/109-2017 (заключний). № держреєстрації 0117U003916. ХНУРЕ. - 116с.;
  + «Методи, системи та засоби кріптографічного захисту інформації з гарантованим рівнем стійкості та підвіщеною швидкодією», Звіт про науководослідну роботу за договором № 295 (заключний). (№ДР 0115U002431);
  + «Створення науково-методичних основ забезпечення живучості мережевих систем обміну інформацією в умовах зовнішнього впливу потужного НВЧ випромінювання», Звіт про науководослідну роботу за договором від 13.04.2018 р. № Ф76/23-2018 (проміжний за 1 етап). № держреєстрації 0118U000832. ХНУРЕ. - 116с.;

**Практичне значення отриманих результатів.** Практична значимість отриманих теоретичних результатів дисертаційної роботи підтверджено ефективністю запропонованої моделі тільки для виявлення аномального поведінки мережного трафіку на основі множини параметрів мережних

з'єднань, що реалізується шляхом аналізу вхідного трафіку за допомогою ансамблю класифікаторів. Зокрема, практичне вирішення теоретичних досліджень полягає у наступному:

запропонована методика моніторингу, яка визначає умови і порядок оцінки стану РКС за допомогою розробленої мультиагентної системи моніторингу.

запропонована архітектура системи моніторингу з використанням автономних програмних агентів. Архітектура передбачає динамічне формування ієрархічної структури, вузлом якої може виступати будь-яка сутність, що визначається джерелом даних або сенсором. Таким чином, стосовно моніторингу РКС можуть існувати метрики грід, кластерів, обчислювальних вузлів і завдань.

Для взаємодії між усіма агентами пропонується використовувати групу інтелектуальних агентів запиту метою яких є координація агентів збору інформації, реструктуризація отриманої інформації і реалізація протоколів і механізмів передачі повідомлень між усіма агентами моделі.

Введення таких агентів і програмна реалізація стандартизованих інтерфейсів взаємодії між ними дозволяють використовувати спільно на різних рівнях програмне забезпечення незалежних розробників. Наприклад, сенсорами можуть виступати файли даних. Але, всі сенсори формують єдину структуру метрик, однаково доступну різним компонентам СМ.

Таким чином, побудована за даною архітектурою система моніторингу може працювати паралельно з уже розгорнутими засобами моніторингу, заміщаючи їх на деяких рівнях, що дозволяє змінювати і розширювати набір доступних функцій цих систем.

Результати дисертаційної роботи впроваджено у державному підприємстві «Центральне конструкторське бюро «ПРОТОН»», м. Харків (акт від 30.05.18) та Харківському національному університеті радіоелектроніки, кафедра електронних обчислювальних машин, м. Харків в

процесі проведення лекційних занять і лабораторних робіт з курсу

«Технології виявлення загроз в комп’ютерних мережах».

**Публікації**. Матеріали дисертації достатньо повно викладені у 13 роботах: з них 6 статей у виданнях, які зазначені в переліку фахових видань України з технічних наук [1-6] (всі праці входять до науково-метричних баз, 2 – до бази Scopus ) та 7 тез доповідей міжнародних конференцій [7-13 ] (1 – до бази Scopus ).

ВИСНОВКИ

У дисертаційній роботі вирішена актуальна наукова задача покращення показників виявлення аномалій функціонування РКС в умовах кібернетичних впливів зовнішнього та внутрішнього середовища шляхом побудови моделей і методів на основі технологій інтелектуального аналізу даних.

Основні результати виконаної роботи полягають в наступному:

* + 1. Проведено аналіз існуючих методів і засобів моніторингу розподілених інформаційних систем, який виявив відсутність надання цілісної оцінки стану функціонування РКС.
    2. Розглянуто особливості архітектури розподілених комп’ютерних систем, що дозволило виявити базові компоненти розподілених комп’ютерних систем, які потребують постійного моніторингу їх стану.
    3. Визначено множину параметрів для оцінки стану кожного елемента системи, що дає можливість для подальшої оцінки функціонування системи в цілому та скоротити час навчання ансамблю класифікаторів на 30,79%.
    4. Розроблено метод виявлення аномалій в мережі на основі стекінгу методів інтелектуального аналізу даних, який на відміну від існуючих алгоритмів виявлення аномалій дозволяють підвищити точність виявлення до 92,7% і знизити кількість помилкових другого роду до 4,05% за рахунок використання різнорідних методів інтелектуального аналізу даних і до навчання системи на даних підчас роботи системи моніторингу.
    5. Розроблено структура та архітектура системи моніторингу з використанням автономних програмних агентів. Архітектура СМ призначених для вирішення завдань збору та зберігання параметрів отриманих від датчиків, що характеризуються не тільки їх цільовими функціями, але і функціональними можливостями.
    6. Розроблено методику та комплекс моделей процесу функціонування мультиагентної системи моніторингу аномалій при функціонуванні компонентів РКС, що базуються на методології IDEF0, що деталізують процес моніторингу стану РКС и дозволяють інтегрувати систему моніторингу з іншими компонентами системи захисту інформації.
    7. Розроблено програмний комплекс дослідницького прототипу системи моніторингу аномалій функціонування РКС. Ефективність розробленої системи моніторингу підтверджена методом імітаційного моделювання атак на сегмент мережі РКС. Прототип забезпечує ймовірність прийняття вірного рішення про наявність аномального трафіку склало 97%, помилки першого роду - 2% і помилки другого роду - 1%.

Достовірність нових наукових положень дисертаційної роботи підтверджена результатами практичного впровадження методів та інструментальних засобів підтримки процесу оцінювання та забезпечення кібербезпеки функціонування комп’ютерних систем.

Подальші дослідження доцільно спрямувати на вдосконалення та покращення методу оцінки стану обчислювального вузла та стану запущених завдань в комп’ютерній системі.