Голові спеціалізованої вченої ради Д 26.062.17
при Національному авіаційному університеті
03058, м. Київ, просп. Космонавта Комарова, 1

ВІДГУК
офіційного опонента

начальника кафедри захисту інформації та кібербезпеки Житомирського військового інституту імені С. П. Корольова доктора технічних наук, професора Грищука Руслана Валентиновича на дисертацію Петренка Тараса Анатолійовича "Методи та моделі експертних систем розпізнавання кібератак на основі кластеризації ознак", поданої ним на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації

Актуальність теми

Системи захисту інформації (СЗІ) відіграють надзвичайно важливу роль в сучасній архітектурі інформаційно-телекомунікаційних систем. На них покладаються функції з моніторингу трафіку з подальшим виявленням та класифікацією мережних аномалій. Задачі такого класу є тривіальними. У своїй більшості вони успішно вирішуються шляхом своєчасного оновлення бази даних сигнатур шкідливого програмного забезпечення в обраній СЗІ. Такий підхід, як показала практика, хоч і має місце, але він завідомо на крок програє в ефективності у відношенні до кібератак на які ще такі сигнатури не створені. Тому застосування так званих "пасивних" СЗІ на об'єктах критичної інформаційної інфраструктури держави ставить під загрозу безперебійне функціонування як окремих її складових – інформаційних та телекомунікаційних систем, так і інформаційно-телекомунікаційних систем в цілому.

Альтернативою описаному вище підходу є підхід, що ґрунтується на створенні "проактивних" СЗІ в основу функціонування яких покладено технології інтелектуального розпізнавання кібератак. В умовах невизначеності класу та типу кібератак, які потенційно можуть мати місце і сигнатури на які ще не створено, першим завданням, що повинно вирішуватися проактивною СЗІ після виявлення кібератаки, є її розпізнавання за визначеними ознаками. Але недосконаліть відомих моделей та методів розпізнавання кібератак суттєво стримує створення нового класу проактивних інтелектуальних СЗІ в інформаційно-телекомунікаційних системах. *Отже, зважаючи на зв'язок теми дисертації Петренка Т. А. з означеними вище питаннями, вважаємо її достатньо обґрунтованою та актуальною.*

Оцінка обґрунтованості наукових положень, висновків та рекомендацій, сформульованих у дисертації, їх достовірність, новизна

Загальна характеристика дисертації

У **вступі** здобувачем подано загальну характеристику роботи, обґрунтовано актуальність обраної теми, сформульовано мету і завдання дослідження, відображено наукову новизну й практичну цінність одержаних результатів, наведено дані щодо їх апробації та впровадження.

вх. 0306/2019
від 20.06.2019 р.

У **першому розділі** здобувачем проведено аналіз методів та моделей розпізнавання кібератак на критично важливі інформаційні системи. За результатами аналізу *встановлено*, що для підвищення ефективності розпізнавання кібератак слід обирати непересічні ознаки, які характеризують той чи інший клас кібератак з подальшим обґрунтуванням функції близькості та критерію розбиття на відповідні множини. *Обґрунтовано* доцільність вирішення означеної вище задачі на основі моделей та методів кластерного аналізу. Далі, що цілком логічно, *проаналізовано* відомі методи і моделі, які на сьогодні використовуються для побудови інтелектуального розпізнавання кібератак в СЗІ. *Показано*, що такі методи і моделі хоча і мають місце, але потребують удосконалення в частині, що стосується формування раціональної кількості ознак кібератак для відповідного класу кіберзагроз. *Таким чином, результатом першого розділу є формалізація задач, які потребують вирішення і вирішуються в дисертації.*

У **другому розділі** розроблено модель адаптивної системи інтелектуального розпізнавання кібератак з використанням процедури нечіткої кластеризації реалізації ознак. В основу моделі, як *показано* у розділі, покладено ідею багатоетапного виявлення загроз, аномалій і кібератак, що *дозволило визначити* роль та місце створюваної адаптивної системи інтелектуального розпізнавання. Коректно *сформульовано* вимоги до методу та моделі інформаційного синтезу адаптивних та здатних до самонавчання адаптивних систем розпізнавання. *Позитивною* стороною розробленої моделі є те, що здобувач не тільки формулює припущення у ході розроблення моделі, а й зазначає які саме первинні та вторинні реалізації ознак об'єктів розпізнавання можуть бути використані практично. Такий підхід суттєво підкріплює *адекватність* розробленої моделі.

Для оцінювання ефективності процесу машинного навчання у другому розділі *обрано* відповідні інформаційні критерії такі, як ентропія та критерій Кульбака-Лейблера. Зазначене *дозволило*: з одного боку врахувати технічний стан критично важливої інформаційної системи, з іншого – врахувати достатньо велику кількість даних, які підлягають оцінюванню в ході навчання системи. *Таким чином, як результат, у другому розділі закладено науково обґрунтований базис для створення адаптивних систем розпізнавання кібератак з коректними вирішальними правилами.*

Третій розділ дисертації здобувач присвятив розробленню методів кластеризації та оптимізації контрольних допусків на реалізацію ознак розпізнавання кібератак. Зокрема було *запропоновано* метод кластеризації реалізації ознак при виявленні складних кібератак. *Удосконалено* принцип кластеризації в основу якого покладено ідею збільшення радіусу контейнера об'єктів розпізнавання на кожному кроці навчання. *Доведено*, що навчання експертної системи є ітераційною процедурою, зупинник якої спрацьовує у разі досягнення максимуму інформаційного показника функціональної результативності. Такий показник також розроблено та подано у розділі. Акцентовано увагу на тому, що остаточний вибір варіанта рішення на початковому етапі пошуку керуючих впливів в ході навчання експертної системи, що забезпечують оптимальні значення інформаційного показника функціональної результативності, перевіряється експертами з інформаційної безпеки. Таким чином, здобувачем через вирішальні правила *вперше* встановлено зв'язок між станами

критично важливих інформаційних систем та класами кібератак, які мають місце в таких системах. Результати імітаційного моделювання приведені у даному розділі наочно доводять достовірність розробленого методу. *Отже, основним результатом, який здобувач одержав у третьому розділі є метод, що дозволяє підвищувати результативність кластеризації ознак при виявленні складних кібератак.*

Четвертий розділ в дисертації є заключним. Його присвячено питанням експериментальних досліджень адаптивної експертної системи розпізнавання кібератак. Зокрема, *коректно*, як на наш погляд, визначено вихідні дані та методику проведення досліджень, *формалізовано* модель процесу організації та проведення експерименту. *Описано* хід проведення експерименту за етапами та *критично проаналізовано* одержані результати. *Показано та описано* інтерфейсну частину розробленої експертної системи, *розкрито* її основні функціональні можливості. Показані приклади практичного застосування.

У **висновках** приведено основні одержані результати, їх наукову та практичну цінність.

У **додатках** до дисертації наведено: копії актів, які підтверджують впровадження роботи; лістинг розробленої експертної системи;

Сформульовані в дисертації наукові положення, висновки та рекомендації достатньо повно обґрунтовані здобувачем та викладені в доказовій формі.

Наукова новизна одержаних особисто здобувачкою результатів полягає у такому.

Вперше:

– розроблено модель експертної системи у складі інтелектуальних систем виявлення вторгнень, у якій реалізовано процедуру нечіткої кластеризації реалізацій ознак кібератак та наступну корекцію вирішальних правил, що дозволяє створювати адаптивні механізми самонавчання систем інтелектуального розпізнавання кібератак;

– запропоновано застосовувати в якості оціночного показника ефективності навчання експертної системи модифіковану інформаційну умову функціональної результативності, яка ґрунтується на ентропійному та інформаційно-дистанційному критерії Кульбака – Лейблера, що дозволяє отримувати вхідну навчальну матрицю, яка використовується як об'єкт навчання, й будувати коректні вирішальні правила розпізнавання кібератак на критично важливі інформаційні системи.

Удосконалено:

– метод розбиття простору реалізацій ознак на кластери в ході реалізації процедури розпізнавання кібератак, який відрізняється від існуючих, одночасною оптимізацією при обчисленні контрольних допусків у ході аналізу експертною системою складних реалізацій ознак об'єктів спостереження, та дозволяє на кожному кроці навчання змінювати перевірочні допустимі відхилення для всіх реалізацій ознак кібератак одночасно;

– метод навчання експертної системи, який являє собою ітераційну процедуру пошуку глобального максимуму інформаційної умови функціональної результативності, та, на відміну від існуючих, дозволяє попереджати можливі випадки поглинання одним класом об'єктів розпізнавання базових реалізацій ознак іншого класу, враховує відомі статистичні параметри кластеризації реалізацій ознак об'єктів спостереження, а також помилки під час завдання на прийняття рішення в ході процедур машинного навчання.

Набули подальшого розвитку:

– імітаційні моделі для композитної побудови систем інтелектуального виявлення кібератак за рахунок одночасної оптимізації контрольних допусків в ході аналізу об'єктів розпізнавання, що дозволяє проводити їх дослідження, здійснювати вибір раціональних способів протидії і нейтралізації наслідків, аналізувати більш складні і раніше невідомі види кібератак на критично важливі інформаційні системи.

Достовірність наукових положень

Достовірність наукових положень дисертаційної роботи підтверджується:

– коректною постановкою наукового завдання та часткових наукових задач дисертаційного дослідження (с. 47–48 дисерт. та с. 2 автореф.);

– використанням в роботі теоретично обґрунтованих та широко апробованих на практиці методів теорії захисту інформації та кластерного аналізу, методів прикладної статистики, оптимізації та комп'ютерного моделювання, моделі інтелектуальних технологій машинного навчання, методів теорії нечітких множин, методів об'єктно-орієнованого програмування, методології тестування на захищеність;

– збіжністю результатів моделювання та експериментальних перевірок з відомими експериментальними даними інших академічних досліджень, відповідністю отриманих теоретичних результатів з результатами експерименту (с. 159–171, дисерт., с. 14–16, автореф.);

– відповідністю наукових положень основним законам і явищам природи.

Наукове значення дисертаційної роботи полягає в подальшому розвитку теорії захисту інформації в частині, що стосується створення методів та моделей інтелектуальних систем захисту інформації.

Практичне значення дисертації полягає в створенні програмних модулів діючої експертної системи "*Analyzer of cyberthreats*", що реалізують процедуру інтелектуального розпізнавання кібератак на основі кластеризації ознак.

Практична значущість одержаних результатів і достовірність наукових положень підтверджені актами впровадження, копії яких наведено у дисертації (с. 200–202) і про що зазначено в авторефераті на с. 3, що підтверджують особистий внесок здобувача в науку.

Мова та стиль викладення дисертації та автореферату дозволяють зрозуміти суть розроблених наукових положень і одержаних практичних результатів. Дисертація і автореферат у цілому відповідають вимогам, які висуваються до його оформлення відповідно до Порядку присудження наукових ступенів, затвердженого постановою Кабінету Міністрів України від 24.07.2013 р. № 567 (із змінами) та Вимог до оформлення дисертації, затверджених наказом Міністерства освіти і науки України від 12.01.2017 р. № 40. Зміст дисертації та автореферату викладено послідовно та логічно. Поряд з тим не можна не відмітити деякі граматичні та стилістичні неточності, які мають місце в роботі. Наприклад, с. 2, 23, 84 дисертації.

Підтвердження повноти викладу основних результатів дисертації в опублікованих працях

За напрямом дисертаційного дослідження здобувачем опубліковано 16 наукових праць. У тому числі: 2 наукові статті в міжнародних рецензованих виданнях, що входять до наукометричної бази даних *Scopus*, 1 наукова стаття у наукових журналах інших держав, 3 статті у вітчизняних наукових журналах, які входять до інших

міжнародних наукометричних баз даних, 10 матеріалів та тез доповідей на всеукраїнських та міжнародних конференціях.

Перераховані публікації з достатньою повнотою відбивають наукові та практичні результати дисертації. З праць, що їх опубліковано у співавторстві, у дисертації використано лише ті результати, які отримано здобувачем самостійно.

Зауваження щодо змісту дисертації та її оформлення

До основних недоліків дисертаційної роботи можна віднести такі.

1. У вступі до дисертації та далі за текстом здобувач оперує рядом категорій таких, як інформаційно-комунікаційне середовище, критично-важлива інформаційна система, система розпізнавання кіберзагроз тощо. Незрозуміло для чого без обґрунтування вводити нові категорії, якщо вони вже введені і визначені рамками національного законодавства та є загальноприйнятими в кібербезпеці та в системах захисту інформації. Наприклад, це кіберпростір, критично важливі об'єкти інфраструктури, системи виявлення вторгнень тощо.

2. У першому розділі здобувач досить аргументовано описує роль та місце своїх дисертаційний досліджень в загальній проблемі розпізнавання кібератак. Але на наш погляд ті статистичні дані, які приводяться як аргументи, наприклад на с. 23, 24, 26 та 28, є дещо застарілими та потребують більш ретельного обґрунтування. Наприклад, за відсутності достовірних даних на 2017-2019 р.р. можна було б побудувати тренд й проаналізувати його динаміку. Це як мінімум виглядало б більш коректно, порівняно з тим, як подано дані здобувачем. Те саме стосується й кібератак, які мали місце в Україні після 2015 р.

Даний недолік в авторефераті відсутній.

3. Не можна погодитися зі здобувачем в тім, що при узагальненні даних про методи, які використовуються у сучасних системах розпізнавання кібератак (мається на увазі системах виявлення вторгнень) можна ототожнювати такі наукові категорії як метод і модель, як це зроблено у табл. 1.4. У даному випадку, на наш погляд, слід було б добавити ще один стовбець у таблиці, чим виокремити методи від моделей.

4. Приведена у другому розділі дисертації в якості прикладу схема роботи багатоетапної системи інтелектуального розпізнавання кібератак (рис. 2.2) в частині, що стосується опису етапів атаки має досить узагальнений характер. Будь-яка кібератака, не зважаючи на їх різноманіття, складність, специфіку тощо, в класичному розумінні має однакову таксономію. Тому формально зазначивши на схемі етап атаки 1 чи етап атаки 2 мають бути дані деякі роз'яснення. Незрозуміло, за який саме етап іде мова: розвідку, проникнення та далі за текстом, оскільки на різних етапах здійснення кібератаки застосовуються різні техніки, засоби та й в цілому різна методологія.

5. Важливим питанням при створенні експертних систем, у тому числі й експертних систем, як елементів сучасних систем захисту інформації, є питання оцінювання функціональної ефективності процесу машинного навчання. Справедливо відмітимо, що даний факт у дисертації та авторефераті відзначає й сам здобувач. Але на наш погляд до вирішення даного питання здобувач підійшов досить безапеляційно, запропонувавши в якості інформаційної міри застосовувати ентропійну міру та

критерій Кульбака-Лейблера. Якщо з ентропійною мірою, яка опосередковано описує технічний стан "критично важливої інформаційної системи" погодитися можна, то введення критерію Кульбака-Лейблера потребує додаткового обґрунтування. Наприклад, які дані буде отримано на основі даного критерію, якщо експертна система буде не в змозі ні розпізнати, ні не розпізнати кібератаку. Інколи в системах захисту інформації такі помилки називають помилками третього роду.

6. У дисертації визначення ступеня приналежності "найкращому" варіанту Парето-оптимального нечіткого рішення при формуванні бази знань для експертної системи (с. 116 дисерт., с. 11 автореф. відповідно) в методі кластеризації реалізацій ознак, виконано із застосуванням критерію Вальда і критерію Севіджа. Здобувач при цьому стверджує, що рішення, яке прийматиме експерт або експертна система буде Парето-оптимальним. При цьому здобувач не наголошує, якій підмножині з Парето-оптимальних рішень воно належатиме – області згоди, чи області компромісів. Дане питання принципове, оскільки остання з підмножин, враховуючи великі об'єми даних, які обробляються експертною системою та їх динамічність, є бажаною.

7. При імітаційному моделюванні адаптивної системи інтелектуального розпізнавання із використанням процедури нечіткої кластеризації та паралельної оптимізації контрольних відхилень для реалізацій ознак кібератак, здобувач, як приклад, наводить скріншот інтерфейсу *Wireshark*. При цьому він не зазначає для якого класу мережних кібератак даний приклад. Так, на перший погляд, може скластися враження, що автором роботи проведено моделювання для всіх відомих класів кібератак. Але виходячи з аналізу протоколу *LLMNR,* прописаного в інтерфейсному вікні *Wireshark,* стає зрозуміло те, що: по-перше, моделювання проведено в локальній мережі; по-друге, здобувачем в якості операційної системи використано сімейство операційних систем *Windows*; по-третє, як наслідок, дані зібрані для атак типу U2R. Виникають цілком природні запитання: з якими показниками якості функціонуватиме адаптивна система інтелектуального розпізнавання в глобальній мережі; які вхідні дані матимуть місце для інших операційних систем; як система реагуватиме на кібератаки *Proba, R2L* та *DOS*.

8. У четвертому розділі здобувач приводить результати порівняння відомих та розроблених методів виявлення вторгнень. При цьому вхідні вибірки обирає за базою даних KDD-99 за різної кількості вхідних даних. В одному випадку – для відомих моделей використовує увесь набір вхідних параметрів, а саме – 41, при апробації своїх методів використовує усічену вибірку – 10-12 параметрів, демонструючи при цьому виграш майже за усіма класами кібератак. Це я мінімум некоректно, оскільки вхідний набір при порівнянні повинен бути, як мінімум співвимірним, а не відрізнятися в середньому в 3,8 рази. У такому випадку для порівняння слід було скористатися іншими відомими методами виявлення вторгнень, які оперують такою ж кількістю вхідних параметрів. Такі методи відомі та доступні з відкритого друку.

9. У дисертації, наприклад у додатку, хотілося б побачити рекомендації з практичного застосування розробленої експертної системи. Іншими словами – інструкцію користувачу, яка б містила всю інформацію, необхідну для повноцінної роботи з такою системою. Даний недолік несе більш рекомендаційний характер та має

на меті акцентувати увагу саме на прикладному характері одержаних результатів, що без сумніву є перевагою роботи.

Таким чином, зазначені недоліки дещо впливають на якість подання дисертації, але їх наявність не знижує практичної, а тим паче наукової цінності одержаних здобувачем результатів.

Висновки

Отже, на основі критичного вивчення дисертації, автореферату дисертації та праць здобувача, опублікованих за темою дисертації, об'єктивно **встановлено:**

– дисертаційна робота Петренка Т. А. відповідає вимогам Порядку присудження наукових ступенів, затвердженого постановою Кабінету Міністрів України від 24.07.2013 р. № 567 (із змінами);

– дисертаційна робота відповідає п. 1 паспорту спеціальності 05.13.21 – системи захисту інформації;

– зміст автореферату ідентичний основним положенням дисертації;

– використання чужих наукових результатів без посилань на авторів у дисертації не виявлено, що свідчить про особистий внесок здобувача в науку;

– дисертація Петренка Т. А. є завершеною кваліфікаційною науковою працею, що місить нові науково обґрунтовані результати проведених здобувачем досліджень, які розв'язують конкретне наукове завдання, пов'язане з підвищенням ефективності систем інтелектуального розпізнавання кібератак на критично важливі інформаційні системи на основі розроблених методів та моделей експертних систем, що ґрунтуються на принципах розпізнавання та кластеризації кібератак. Дане наукове дослідження має істотне значення для подальшого розвитку теорії та практики захисту інформації й створення інтелектуальних систем захисту інформації;

– автор дисертації, ПЕТРЕНКО Тарас Анатолійович заслуговує на присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації.

Офіційний опонент –
начальник кафедри захисту інформації та кібербезпеки
Житомирського військового інституту імені С. П. Корольова

доктор технічних наук, професор Р. В. ГРИЩУК

"11" червня 2019 р.

Підпис професора ГРИЩУКА Р. В. засвідчую.
ТВО начальника відділу персоналу та стройового
В. Ю. КІСЕЛЬОВ