ВІДГУК

офіційного опонента про дисертаційну роботу
ПОГОРЕЛОВА Володимира Володимировича
«Нейромережеві моделі та методи розпізнавання комп'ютерних вірусів»
представлену на здобуття наукового ступеня кандидата технічних наук за
спеціальності 05.13.21 – «Системи захисту інформації»

Актуальність теми. В наші дні зловмисники використовують автоматизований підхід до атак, і антивірусам важко захищати системи застарілими методами, тому сьогодні виникає актуальна задача розробки ефективних нейромережевих моделей та методів розпізнавання комп'ютерних вірусів, адаптованих до умов вітчизняних систем антивірусного захисту. З огляду на це, сучасні системи антивірусного захисту є одним з основних засобів захисту інформації більшості комп'ютерних систем і мереж. Не зважаючи на те, що такі системи використовуються вже не одне десятиліття і їх розробкою та створенням методологічної бази займаються висококваліфіковані фахівці, практичний досвід і результати багатьох науково-практичних досліджень вказують на наявність в сучасних антивірусах розпізнавання суттєвих недоліків. Основним з яких є недостатня точність розпізнавання всієї номенклатури комп'ютерних вірусів, що підтверджується відомими випадками успішних вірусних кібератак на вітчизняні та закордонні комп'ютерні системи і мережі. Однак впровадження відомих засобів розпізнавання комп'ютерних вірусів в вітчизняні системи захисту інформації викликає необхідність їх складної адаптації до очікуваних умов використання. Також недоліками відомих засобів розпізнавання є висока вартість і відсутність докладної науково-технічної документації. Важливим напрямком підвищення точності розпізнавання є «інтелектуалізація» методів розпізнавання за рахунок використання теорії штучних нейронних мереж. Перспективність вказаного напрямку підтверджується окремими вдалими застосуваннями нейронних мереж в засобах розпізнавання комп'ютерних вірусів. Разом з тим, недостатня точність

розпізнавання та недостатня адаптованість до умов експлуатації, закритість використаних рішень, значно обмежують сферу їх застосування. При цьому постійний прогрес в області теорії нейронних мереж вказує на можливість значного вдосконалення апробованих засобів розпізнавання. Саме цій проблематиці присвячено дане дисертаційне дослідження.

Зв'язок роботи з науковими програмами, планами, темами. Тематика дисертаційної роботи та одержані результати безпосередньо пов'язані з «Основними науковими напрямами та найважливішими проблемами фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук НАН України на 2019-2023 роки», зі Стратегією кібербезпеки України від 15 березня 2016 року №96/2016. Результати роботи відображені у звітах держбюджетних науково-дослідних робіт Національного авіаційного університету «Квантово-криптографічні методи захисту критичної інформаційної структури держави», «Системи мультирівневого розмежування доступу до інформаційних ресурсів» та «Дослідження ризиків інформаційної безпеки об'єктів критичної інфраструктури ГТС України та розробка методології поводження з ними».

Мета і задачі дослідження. Метою дисертаційної роботи є підвищення ефективності протидії комп'ютерним вірусам за рахунок розробки і дослідження нових нейромережевих моделей, методів і засобів розпізнавання комп'ютерних вірусів, здатних оперативно пристосовуватись до умов використання і реагувати на виникнення нових видів вірусів.

Відповідно до поставленої мети визначено такі основні завдання дослідження:

– проведення аналізу можливостей нейромережевих засобів (НМЗ) розпізнавання комп'ютерних вірусів;

– розробка моделі формування параметрів та концептуальної моделі оцінювання глибоких нейронних мереж (ГНМ);

– розробка методу визначення архітектурних параметрів глибокої нейронної мережі та розвиток методу розпізнавання комп'ютерних вірусів;

– проведення експериментальних досліджень, спрямованих на верифікацію запропонованих рішень.

Об'єктом дослідження є процеси розпізнавання комп'ютерних вірусів.

Предметом дослідження є нейромережеві моделі та методи розпізнавання комп'ютерних вірусів.

Методи дослідження. Використано методи теорії захисту інформації, НМ, комп'ютерного моделювання, експертного і статистичного аналізу та оптимізації.

Ступінь обґрунтованості положень висновків та рекомендації, що проведені в роботі, повністю відображаються та підтверджуються отриманими результатами, що приведені в роботі, описами процесу розв'язку задач, які представлені в основному змісті роботи, та обґрунтовуються коректною методикою послідовного та повного висвітлення отриманих у роботі результатів.

Достовірність отриманих нових результатів при розв'язку поставлених задач підтверджується коректним використанням формальних засобів опису основних елементів предмету дослідження та повною узгодженістю задач, що розв'язуються в роботі.

Наукова новизна отриманих результатів. Проведені у дисертаційній роботі дослідження дозволили розробити й науково обґрунтувати принципи, моделі та методи нейромережевого розпізнавання комп'ютерних вірусів.

1. Вперше розроблено концептуальну модель оцінювання глибоких нейронних мереж, яка за рахунок взаємопов'язаних принципів допустимості використання, визначення множини ефективних видів та оцінювання ефективності виду глибокої нейронної мережі дозволяє визначити множину сучасних нейромережевих моделей для побудови ефективних антивірусних засобів;

2. Вперше розроблено модель формування параметрів навчальних прикладів глибокої нейронної мережі, яка за рахунок формального представлення закодованих значень викликів API-функцій, байт-послідовності N-грамів, опкодів, основних регістрів процесора, а також результатів статичного аналізу зразків шкідливих та безпечних програм, двомірної інтерпретації

бінарного коду програми і параметрів графу залежностей значень та станів дозволяє будувати засоби нейромережевого аналізу обфускованого програмного коду;

3. Вперше розроблено метод визначення архітектурних параметрів глибокої нейронної мережі, призначеної для розпізнавання вірусів, який за рахунок використання запропонованої концептуальної моделі оцінювання глибоких нейронних мереж та моделі формування параметрів навчальних прикладів, що використовуються для реалізації етапів визначення основних умов застосування, доцільності використання нейромережевої моделі та найбільш ефективної архітектури, а також формування параметрів навчальних прикладів та визначення параметрів архітектури найбільш ефективного виду глибокої нейронної мережі, дозволяє сформувати набір величин, які забезпечують пристосованість такої мережі до визначених умов застосування;

4. Отримав подальший розвиток метод нейромережевого розпізнавання комп'ютерних вірусів, який, за рахунок визначення умов створення та застосування нейромережевих засобів, процесів формування портретів вірусів та безпечних програм, а також визначення архітектурних параметрів глибокої нейронної мережі та верифікації і оцінки ефективності нейромережевих засобів, забезпечує достатню похибку розпізнавання при різних умовах застосування з урахуванням обмежень щодо створення навчальної вибірки та обмежень щодо обчислювальних ресурсів системи антивірусного захисту.

Практичне значення одержаних результатів дисертаційного дослідження полягає у наступному:

1. Розроблене алгоритмічне та програмне забезпечення, що базується на створених нейромережевих методах та моделях, дозволило забезпечити достатню точність розпізнавання комп'ютерних вірусів та приблизно в 1,5 рази зменшити обчислювальні витрати, пов'язані з визначенням значень архітектурних параметрів ГНМ, що підтверджується актом впровадження в діяльність ТОВ «Сайфер ПРО».

2. Розроблені програми, що реалізують запропоновані моделі та методи, впроваджені в навчальний процес на кафедрі безпеки інформаційних технологій Національного авіаційного університету.

3. Результати проведених розрахунків вказують на те, що ефективність розробленого НМЗ приблизно в 1,14 рази вища ніж у подібних відомих засобів. Таким чином, результати досліджень підтверджують можливість підвищення ефективності розпізнавання комп'ютерних вірусів за рахунок застосування розроблених нейромережевих моделей (НММ) та НМЗ, що підтверджується актом впровадження в діяльність ТОВ «Сайфер ПРО».

Повнота викладення основних результатів дисертації у наукових фахових виданнях.

Основні наукові положення дисертації опубліковано у 14 наукових працях, серед яких 7 наукових статей (4 статті у фахових наукових виданнях України, 3 – у міжнародних рецензованих виданнях, які входять до бази наукометричної бази даних SCOPUS), 1 закордонна колективна монографія, а також 6 матеріалів і тез доповідей на конференціях.

Видані статті містять основні аспекти наукової новизни за усіма напрямками досліджень. Особистий внесок автора у працях, написаних у співавторстві, приведені у вступах дисертації та автореферату.

Мова та стиль викладення дисертації.

Текст дисертації викладений логічно, послідовно, грамотно, сучасною технічною мовою. Терміни та визначення, які використовує та пропонує автор, відповідають прийнятим у цій галузі науки і чинним нормативним та керівним документам. Автор користується сучасними іноземними джерелами. Незважаючи на незначні недоліки технічного характеру стиль роботи доступний і дозволяє легко сприймати матеріал.

Відповідність змісту автореферату основним положенням дисертації.

Автореферат містить основні положення й результати досліджень і досить повно відображає суть дисертаційної роботи. У вступі обґрунтовано актуальність теми дисертації, визначено мету і задачі дослідження, розкрито

наукову новизну та практичне значення отриманих результатів, наведені дані щодо їх апробації та впровадження. У першому розділі охарактеризовано науково-прикладну задачу розробки засобів розпізнавання комп'ютерних вірусів в системах антивірусного захисту. Проведено аналіз науково-практичних досліджень, присвячених вирішенню задачі розпізнавання комп'ютерних вірусів. Обґрунтована перспективність застосування в контурі розпізнавання системи антивірусного захисту нейромережевих засобів. Другий розділ присвячено розвитку методологічної бази нейромережевого розпізнавання комп'ютерних вірусів. Третій розділ присвячено розробці нейромережевої моделі та методів розпізнавання комп'ютерних вірусів. Четвертий розділ присвячено практичній реалізації та експериментальним дослідженням розроблених рішень. Розроблено методику проведення експерименту, обґрунтовано доцільність вибору бази експерименту, визначено мету та задачі експерименту, вхідні та вихідні параметри, гіпотезу і критерії дослідження, достатність експериментальних об'єктів та послідовність необхідних дій. У додатках вміщено акти впровадження результатів дисертаційної роботи та фрагменти кодів програм, що відображають практичну частину дисертаційного дослідження.

Зауваження та недоліки дисертаційної роботи.

До основних недоліків та зауважень дисертації можна віднести такі:

1. У п. 2 наукової новизни (стор. 15 дисертації) автор декларує, що вперше розроблено модель формування параметрів навчальних прикладів глибокої нейронної мережі, яка за рахунок формального представлення закодованих значень викликів API-функцій, байт-послідовності N-грамів, опкодів, основних регістрів процесора, а також результатів статичного аналізу зразків шкідливих та безпечних програм, двомірної інтерпретації бінарного коду програми і параметрів графу залежностей значень та станів дозволяє будувати засоби нейромережевого аналізу обфускованого програмного коду. Проте, навіть після проведених експериментів (п. 4.2) не зрозумілий рівень забезпеченості

нейромережевого розпізнавання обфускованого програмного коду, характерного для сучасних поліморфних вірусів.

2. У результаті проведеного аналізу автором (розділі 1) сучасних нейромережевих моделей та методів розпізнавання комп'ютерних вірусів, зазначена низка недоліків, щодо високої потреби в обчислювальних ресурсах, низької адаптованості до проведення аналізу обфускованого програмного коду та недостатньої ефективності розпізнавання, проте у тексті дисертації та висновках не повною мірою усуваються зазначені недоліки, а також не в повній мірі вказані недоліки сучасних нейромережевих моделей та методів розпізнавання комп'ютерних вірусів.

3. У третьому розділі (стор. 99) автором розроблено метод визначення архітектурних параметрів глибокої нейронної мережі, який забезпечує можливість зменшення обсягу експериментальних досліджень, пов'язаних з визначенням архітектурних параметрів глибокої нейронної мережі, призначеної для використання в нейромережевих засобах розпізнавання комп'ютерних вірусів. Проте, у дисертаційній роботі, доцільно було б детальніше описати яким чином забезпечується можливість підвищення ефективності нейромережевих методів розпізнавання комп'ютерних вірусів.

4. У розділі 4.3 (стор. 135) для навчання та тестування ГНМ використовується опублікована компанією Microsoft БД комп'ютерних вірусів BIG-2015. Вказана БД дозволена для вільного використання в науково-практичних цілях для вирішення задач підвищення ефективності засобів антивірусного захисту комп'ютерних систем, проте на мій погляд коректніше було б використати аналогічні БД, а одержані при цьому результати доцільно було б привести у вигляді порівняльної таблиці.

5. Методика проведення експериментального дослідження (розділ 4), не досить повно й чітко формалізована, що ускладнює розуміння умов, в яких проводились експерименти – на яких комп'ютерах (мережах), з якими обчислювальними потужностями, операційними системами тощо.

6. Деякі рисунки та графіки у дисертації відображено з поганою якістю, що ускладнює їх загальне розуміння.

7. Дисертаційна робота та автореферат містять велику кількість скорочень, абревіатур, надписів англійською мовою та формул великого розміру, що значно ускладнює загальний процес оцінки при читанні.

Зроблені зауваження не впливають на загальний високий науковий рівень дисертації та не піддають сумніву основні наукові результати, отримані здобувачем.

Висновок про дисертацію в цілому та її відповідність встановленим вимогам.

Дисертаційна робота Погорелова В.В. є завершеною науковою працею в якій отримано нові наукові результати. Вирішене актуальне наукове завдання, наукова новизна основних положень і практична спрямованість отриманих результатів з їх впровадженням мають суттєве значення для подальшого розвитку систем захисту інформації. Таким чином, дисертаційна робота Погорелова В.В. відповідає усім вимогам, які висуваються до кандидатських дисертацій.

Вважаю, що за своєю актуальністю, ступенем новизни та обґрунтованістю отриманих наукових результатів дисертаційна робота відповідає вимогам «Порядку присудження наукових ступенів», затвердженого постановою Кабінету Міністрів України від 24 липня 2013 року № 567 (зі змінами, внесеними згідно з Постановами КМУ № 656, від 19.08.2015 р., № 1159 від 30.12.2015 р., № 567 від 27.07.2016 р.), а її автор Погорелов Володимир Володимирович заслуговує присудження йому наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації».

Офіційний опонент:

кандидат технічних наук
асистент кафедри кібербезпеки та захисту інформації
факультету інформаційних технологій
Київського національного університету
імені Тараса Шевченка Фесенко А.О.

Підпис Фесенко А.О.
Вчений секретар НДЧ
Караульна І.В.
16.11.2020р.