Голові спеціалізованої вченої ради Д 26.062.17
при Національному авіаційному університеті
03058, м. Київ, пр. Любомира Гузара, 1.

**ВІДГУК**

офіційного опонента – професора кафедри захисту інформації Національного університету «Львівська політехніка»
доктора технічних наук, доцента Опірського Івана Романовича,
на дисертацію Погорелова Володимира Володимировича за темою
«Нейромережеві моделі та методи розпізнавання комп'ютерних вірусів»
подану на здобуття наукового ступеня кандидата технічних наук
за спеціальністю 05.13.21 – «Системи захисту інформації»

**Актуальність теми**

Сьогодні 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 (антивірус з відкритим програмним кодом ClamAV, стартап Deep Instinct) та великою кількістю відповідних теоретико-практичних робіт.

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.

В такій постановці проблеми є актуальною науково-прикладна задача розробки ефективних нейромережевих моделей та методів розпізнавання комп'ютерних вірусів, адаптованих до умов вітчизняних систем антивірусного захисту.

**Ступінь обґрунтованості та достовірності наукових положень, висновків та рекомендацій**

Достовірність та обґрунтованість наукових положень, висновків та рекомендацій забезпечуються коректним вибором методів дослідження, використанням відомого сучасного апробованого математичного апарату, а також тим, що отримані розрахункові результати не суперечать відомим на сьогоднішній день, та мають ясне фізичне трактування. Отримані, під час експериментів, дані відповідають теоретичним висновкам роботи та повністю підтверджують їх. Коректно застосовані методи теорії захисту інформації, комп'ютерного моделювання, експертного і статистичного аналізу та оптимізації.

**Ідентичність змісту автореферату й основних положень дисертації**

У авторефераті дисертації з необхідною повнотою відображено загальну характеристику, основний зміст та висновки дисертації. Структура дисертації відповідає вимогам, які ставляться до кандидатських дисертацій, у тому числі й новим вимогам до оформлення дисертаційних робіт (згідно Наказу Міністерства

освіти і науки України від 12 січня 2017 року № 40). Дисертаційна робота складається зі вступу, чотирьох розділів, висновків та списку використаних джерел (106 найменувань) на 11 сторінках, 2 додатки на 11 сторінках. Загальний обсяг дисертації становить 166 сторінок, у тому числі 144 сторінки основного тексту, ілюстрацій – 38, таблиць – 9.

Результати дисертації викладено послідовно та структуровано, відповідно до поставлених задач дослідження.

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. При цьому показано можливість застосування нейромережевих моделей як в поведінкових аналізаторів, так і при використанні сигнатурного аналізу. Також для вітчизняних систем антивірусного захисту визначена множина очікуваних умов застосування означених нейромережевих засобів.

**Другий розділ** присвячено розвитку методологічної бази нейромережевого розпізнавання комп'ютерних вірусів. Розроблена концептуальна модель оцінювання глибокої нейронної мережі, яка дозволяє визначити множину сучасних нейромережевих моделей для побудови ефективних антивірусних засобів.

**Третій розділ** присвячено розробці нейромережевої моделі та методів розпізнавання комп'ютерних вірусів. Розроблена модель формування параметрів навчальних прикладів глибокої нейронної мережі.

**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.

Варто також зауважити, що для основних положень дисертації та змісту автореферату характерна повна ідентичність.

**Наукова новизна результатів роботи**

На основі аналізу результатів дисертаційної роботи Погорелова В.В., можна зробити висновок, що найбільш суттєвими новими науковими результатами, які одержані ним у дисертації, є такі:

•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;

•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;

•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;

**Практичне значення одержаних результатів дисертаційного дослідження** полягає у наступному:

– 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 глибокої нейронної мережі, що підтверджується актом впровадження в діяльність ТОВ «Сайфер ПРО»;

– розроблені програми, що реалізують запропоновані моделі та методи, впроваджені в навчальний процес на кафедрі безпеки інформаційних технологій Національного авіаційного університету;

– результати проведених розрахунків вказують на те, що ефективність розробленого нейромережевого засобу 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 та нейромережевих засобів, що підтверджується актом впровадження в діяльність ТОВ «Сайфер ПРО».

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».

**Рекомендації щодо використання у дисертації результатів, одержаних автором**

Теоретичні та практичні результати дисертаційної роботи доцільно використовувати в організаціях як приватного, так і державного секторів, а також в науково-дослідних та навчальних установах України, які займаються теоретичними та практичними питаннями, пов'язаними з підвищенням ефективності існуючих та розробленням нових методів та засобів протидії комп'ютерним вірусам. Зокрема, отримані результати можуть бути використані для ефективної побудови нових або розширення функціональних можливостей існуючих систем протидії комп'ютерним вірусам, де важливим є питання працездатності і ефективності системи при обмежених обчислювальних ресурсах.

**Підтвердження повноти викладу основних результатів дисертації в опублікованих працях**

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.

**Зауваження до дисертації та автореферату**

1. У другому розділі дисертаційної роботи автор представив розроблені правила визначення ефективних видів глибоких нейронних мереж (стор.53), які дозволяють уникнути довготривалих комп'ютерних експериментів пов'язаних з формуванням множини допустимих і ефективних видів глибоких нейронних мереж, проте не з роботи і автореферату не зрозуміло, яким чином забезпечується можливість проведення автоматизації такого формування.

2. У дисертаційній роботі на стор. 76 у висновках до другого розділу автор декларує, що у роботі «Вперше розроблено принципи застосування нейронних мереж для розпізнавання комп'ютерних вірусів», що не є дійсністю, по-перше

тому, що застосування нейронних мереж вже здійснювалося для виявлення вірусів і по-друге тому, що вже у наступному реченні автор підкреслює, що «на відміну від відомих у означених принципах відображено…». Наведений пункт висновків необхідно було представити як «удосконалено» або «отримано подальший розвиток» формування принципів нейронних мереж для розпізнавання комп'ютерних вірусів.

3. У третьому розділі представлено метод нейромережевого розпізнавання комп'ютерних вірусів, який забезпечує достатню похибку розпізнавання при різних умовах застосування з врахуванням обмежень щодо створення навчальної вибірки та обмежень щодо обчислювальних ресурсів системи антивірусного захисту. Проте, з результатів експерименту, не зрозуміло рівень похибки та обмежень обчислювальних ресурсів, тому бажано було навести у відповідному місці дисертаційної роботи виграшу кожного із розроблених методів у порівнянні з відомими (аналогами) – це дозволило б більш чітко зрозуміти ступінь новизни кожного з отриманих результатів.

4. У розділі 4.2. автор декларує розроблення експериментальної установки, хоча згідно з опису її основних частин та структури це не є дійсністю, оскільки розроблена система є повноцінною системою і не складається з декількох фізично відокремлених пристроїв або елементів. У цьому випадку правильно було б використати інший термін, наприклад: програмно-апаратний пристрій (засіб), експериментальна комп'ютерна система на основі ПК, програмне забезпечення, алгоритми у вигляді додатків, експериментальна програмно-апаратна комп'ютерна система тощо.

5. У четвертому розділі (стор. 117-142) автором розроблено експериментальну установку (систему), яка забезпечує можливість проведення експериментів, спрямованих на перевірку достовірності основних результатів дисертаційної роботи, проте, результати експериментів, доцільніше було б порівняти з існуючими рішеннями в табличній формі.

6. У розділі 4.3. та у авторефераті на стор.15 автор здійснює тестування розробленої програмної системи за допомогою бази даних комп'ютерних вірусів BIG-2015, проте у самій дисертації та авторефераті ніде не обґрунтовується її

вибір та не представляються альтернативні бази для тестування. Крім того, проведення експериментального дослідження з використанням декількох баз даних могло б підкреслити значущість отриманих результатів і більш наочно продемонструвати переваги розроблених методів і моделей.

7. На стор. 142 автор зазначає, що основним напрямком удосконалення створеної НМС розпізнавання комп'ютерних вірусів є розробка методу для навчання НММ за допомогою експертних правил, проте ні в авторефераті ні в дисертації це твердження не є відображене та обґрунтоване. Наявність такого чіткого обґрунтування підкреслило б шляхи удосконалення систем розпізнавання комп'ютерних вірусів за допомогою нейромереж.

8. Текст дисертації не позбавлений орфографічних помилок та неточностей, наприклад: присутні різні варіанти позначення лапок і тире у тексті дисертації, вкінці немає номерів сторінок чи гіперпосилань, що необхідно відповідно до чинних вимог оформлення списку джерел тощо. А також, дисертаційна робота та автореферат містять велику кількість скорочень, абревіатур та формул – це значно ускладнює загальний процес оцінки результатів роботи при читанні.

**Висновки**

Зазначені у відгуку зауваження не зменшують теоретичної та практичної цінності дисертаційної роботи Погорелова В.В. Загалом, вона характеризується внутрішньою єдністю, виконана на належному науковому рівні та є завершеною працею. В ній отримано нові науково обґрунтовані результати, що в сукупності вирішують науково-практичну задачу 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.

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,**
професор кафедри захисту інформації
Національного університету
«Львівська політехніка»,
доктор технічних наук, доцент Опірський І.Р.

Підпис доцента Опірського І.Р. засвідчую
Вчений секретар Національного університету
«Львівська політехніка», к.т.н., доцент Брилинський Р.Б.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ • НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЛЬВІВСЬКА ПОЛІТЕХНІКА • ЗКПО 02071010