

ВІДГУК

офіційного опонента на дисертаційну роботу

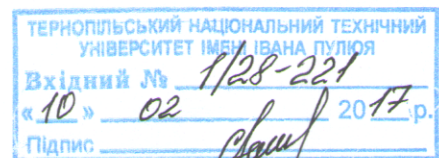
Бобровнікової Кіри Юліївни на тему: «Інформаційна технологія виявлення бот-мереж у корпоративних мережах на основі аналізу DNS-трафіка»,
яка представлена на здобуття наукового ступеня кандидата технічних наук
за спеціальністю 05.13.06 – інформаційні технології

Актуальність теми дисертації. За останні роки кількість шкідливого програмного забезпечення невпинно зростає, і одним з його найбільш небезпечних видів є бот-мережі, боти яких з метою поширення, подолання систем захисту інформаційних систем і протидії виявленню можуть поєднувати в собі функціонал файлових вірусів, мережних черв'яків, троянців та руткітів. Можливість об'єднання з метою здійснення шкідливих дій великої кількості інфікованих комп'ютерів в єдину мережу, керовану зловмисником, перетворює бот-мережі на глобальну загрозу в мережі Інтернет. Відомі інформаційні технології антивірусного діагностування мають низьку достовірність виявлення невідомих ботів бот-мереж, що зумовлює необхідність розроблення принципово нових інформаційних технологій виявлення бот-мереж.

Перспективним напрямком для підвищення достовірності виявлення є використання методів інтелектуального аналізу даних та інтелектуальних інформаційних технологій.

З огляду на це, тема дисертаційної роботи Бобровнікової Кіри Юліївни «Інформаційна технологія виявлення бот-мереж у корпоративних мережах на основі аналізу DNS-трафіка» є **важливою та актуальною.**

Дисертаційна робота безпосередньо пов'язана з планами наукових досліджень, які виконувалися і виконуються на кафедрі «Комп'ютерної інженерії та системного програмування» в рамках держбюджетної НДР Хмельницького національного університету №4Б-2015 «Розвиток наукових та інженерних основ надійності електронної техніки шляхом удосконалення технології її тестування на вібрації та удари».



Оцінка змісту дисертації, її завершеність в цілому та оформлення.

Дисертація є завершеною науково-дослідною роботою. Її структура логічна, оформлена акуратно та згідно встановлених вимог. Автореферат правильно відображає зміст дисертації.

Дисертаційна робота складається зі вступу, чотирьох розділів та висновків, викладених на 150 сторінках основного тексту, списку використаних джерел (138 найменувань). Робота містить 47 рисунків, 7 таблиць та 3 додатки.

У **вступі** обґрунтовано актуальність наукової проблеми та теми дисертаційної роботи, сформульовано мету і задачі, наведено використані методи дослідження, сформульовано наукову новизну та практичну цінність отриманих результатів і показано зв'язок задачі з науковою темою. Наведено дані про впровадження результатів роботи, їх апробацію, публікації та особистий внесок здобувача.

Перший розділ присвячено аналізу методів та засобів, на яких ґрунтуються відомі інформаційні технології виявлення бот-мереж на основі системи доменних імен (DNS) та визначено їх переваги і недоліки. Досліджено достовірність виявлення шкідливого програмного забезпечення найбільш поширеними антивірусними засобами та ефективність їх роботи. Також здійснено постановку задачі.

В **другому розділі** дисертаційної роботи визначено область дослідження та розроблено: модель бот-мереж, яка враховує використання бот-мережами системи доменних імен та застосування технологій ухилення від виявлення; модель DNS-трафіка корпоративної мережі, яка описує основні ознаки, що можуть бути вилучені з DNS-трафіка та вказують на наявність в мережі ботів; модель процесу виявлення бот-мереж на основі аналізу DNS-трафіка, що враховує характерні для бот-мереж особливості поведінки та використання ними технологій ухилення від виявлення. Розроблені моделі є основою для методів виявлення нових та відомих бот-мереж у корпоративних мережах на базі аналізу DNS-трафіка.

У **третьому** розділі розроблено: метод ідентифікації бот-мереж на основі їх групової активності в DNS-трафіку, який використовує нову ознаку синхронності DNS- запитів та враховує характерні для бот-мереж особливості поведінки ботів; метод виявлення бот-мереж, які застосовують технології ухилення від виявлення на основі DNS, що ґрунтується на кластерному аналізі ознак DNS-трафіка та застосовує засоби активного DNS- зондування для уточнення його результатів. Застосування розроблених методів дозволяє підвищити ефективність та достовірність процесу виявлення бот-мереж у корпоративних мережах на основі аналізу DNS-трафіка.

В **четвертому** розділі описані алгоритми виявлення бот-мереж в корпоративних мережах на основі аналізу DNS-трафіка та проведено дослідження їх складності. Розроблено та описано інформаційну технологію виявлення бот-мереж в корпоративних мережах на основі аналізу DNS-трафіка, а також програмні засоби, які реалізують розроблену інформаційну технологію. Проведено порівняльний аналіз достовірності виявлення бот-мереж розробленою інформаційною технологією з відомими, який показав, що використання розробленого програмного забезпечення дозволяє істотно підвищити рівень достовірності виявлення бот-мереж в порівнянні з відомими антивірусними програмними засобами.

У **висновках** сформульовані основні наукові та практичні результати дисертаційної роботи.

В додатках наведено результати досліджень та акти, які підтверджують впровадження результатів дисертаційної роботи.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій та їх достовірність. Достовірність наукових положень і результатів дисертаційної роботи Бобровнікової Кіри Юліївни забезпечується строгістю і коректністю постановок задач та використаного математичного апарату, доведенням теоретичних результатів до розрахунків.

Наукові положення та висновки є новими, достатньо обґрунтованими. В роботі коректно використано математичний апарат. У матеріалах дисертації,

що складають наукову новизну, академічний плагіат відсутній.

Автореферат відповідає основним положенням дисертаційної роботи.

Наукова новизна одержаних у дисертації результатів. До найсуттєвіших нових наукових результатів, отриманих автором особисто, можна віднести:

1) вперше розроблено модель бот-мережі, модель DNS-трафіка та модель процесу виявлення бот-мереж в корпоративних мережах, які засновані на знаннях стосовно ознак DNS-трафіка мережі, що визначаються ключовими особливостями функціонування бот-мереж, зокрема застосування ними методів ухилення від виявлення. Розроблена модель процесу виявлення бот-мереж, на відміну від відомих, залучає нову ознаку синхронності DNS-запитів, що дозволило підвищити достовірність виявлення;

2) вперше розроблено метод ідентифікації бот-мереж у корпоративних мережах на основі їх групової активності в DNS-трафіку, що враховує характерні ознаки функціонування груп інфікованих ботами комп'ютерних систем в мережі, застосовує аналіз значень TTL-періодів DNS, вилучених зі вхідних DNS-повідомлень мережі, враховує нову ознаку синхронності DNS-запитів, що дозволило ідентифікувати як відомі, так і нові боти бот-мереж;

3) вперше розроблено метод виявлення бот-мереж, який здійснює пасивний моніторинг DNS-трафіка та активна DNS-зондування з метою одержання ознак, застосовує кластерний аналіз ознак з частковим навчанням, що дозволило підвищити достовірність ботів в корпоративних мережах;

4) дістала подальшого розвитку інформаційна технологія виявлення бот-мереж в корпоративних мережах на основі аналізу DNS-трафіка, яка, на відміну від відомих аналізує поведінку комп'ютерних систем в DNS-трафіку, що дало можливість виявляти відомі та нові боти бот-мереж та підвищити достовірність виявлення.

– **Практичне значення результатів та їх використання.** Практична цінність роботи полягає в тому, що основні результати дисертації знайшли застосування при програмній реалізації та експлуатації системи виявлення бот-

мереж в мережах на підприємствах ТзОВ «ІТТ - telecommunication company» та ДП «Новатор», що підтверджено актами про впровадження.

Результати дисертаційної роботи Бобровнікової Кіри Юліївни впроваджені в навчальний процес Хмельницького національного університету при викладанні дисциплін «Програмування комп'ютерних мереж», «Технічна діагностика і надійність комп'ютерних пристроїв та систем» та «Інженерія програмного забезпечення», що підтверджено відповідним актом.

Відповідність дисертаційної роботи обраній спеціальності. Робота повністю відповідає паспорту спеціальності 05.13.06 – інформаційні технології, оскільки в ній розроблено нові моделі бот-мережі, DNS-трафіка та модель процесу виявлення бот-мереж в мережах на основі аналізу ознак, які можуть бути вилучені з DNS-трафіка; метод ідентифікації бот-мереж на основі їх групової активності в DNS-трафіку і метод виявлення бот-мереж, які застосовують технології ухилення від виявлення на основі DNS, а також набула подальшого розвитку інформаційна технологія виявлення бот-мереж в корпоративних мережах на основі аналізу DNS-трафіка.

Ідентичність основних положень дисертації і змісту автореферату. Автореферат достатньо повно відображає зміст дисертації та її основні наукові положення і результати.

Висвітлення наукових результатів в опублікованих працях. Наукові результати теоретичних і експериментальних досліджень, викладені в дисертації, одержані автором особисто та опубліковані в 16 наукових роботах, з яких 6 статей в провідних фахових виданнях України, 3 з яких у виданнях, зареєстрованих в науко метричній базі Index Copernicus; 2 публікації – у періодичних закордонних виданнях, зареєстрованих у науко метричній базі Scopus, 1 з яких – у виданні, зареєстрованому в науко метричній базі Web of Science, та 1 – у матеріалах конференцій, індексованих у науко метричних базах Scopus та Web of Science, та 1 патент на корисну модель.

В опублікованих працях в повному обсязі викладено основні результати дисертаційних досліджень.

Оцінка висновків дисертаційної роботи. Висновки до розділів та до дисертаційної роботи в цілому впливають з аналізу розроблених моделей, методів та інформаційної технології виявлення бот-мереж на основі аналізу DNS-трафіка. Усі висновки є обґрунтовані та представляються достовірними.

Недоліки та зауваження по роботі:

1. В дисертаційній роботі приділено мало уваги дослідженню методів кластерного аналізу як засобів антивірусного діагностування комп'ютерних систем на наявність бот-мереж;
2. В дисертаційній роботі не висвітлено оцінку якості моделювання, адекватності розроблених моделей;
3. Не досліджено властивості кластерів, отриманих за допомогою розробленого метода ідентифікації.
4. Не виконано компонентний чи інформаційний аналіз вектора ознак бот - мереж.
5. Твердження «підвищенні точності та інформативності результатів кластеризації» (с.16 автореферату) приведено без експериментальних даних.
6. В авторефераті надано загальний опис моделі процесу виявлення бот-мереж на основі аналізу DNS-трафіка, але не розкрито значення її складових.
7. Мало уваги приділяється дослідженню оперативності розробленої інформаційної технології.

Перелічені зауваження не впливають на загальний науковий рівень і практичну цінність дисертаційної роботи.

Висновки.

1. Дисертаційна робота Бобровнікової Кіри Юліївни «Інформаційна технологія виявлення бот-мереж у корпоративних мережах на основі аналізу DNS-трафіка» є актуальною завершеною науковою працею, яка розв'язує важливу наукову задачу.

2. Автореферат об'єктивно і повно відображає зміст дисертації.
3. Дисертаційна робота Бобровнікової Кіри Юліївни за своїм рівнем, обсягом і якістю досліджень відповідає вимогам «Порядку присудження наукових ступенів і присвоєння вченого звання старшого наукового співробітника», зокрема п. 11, а здобувач заслуговує присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – інформаційні технології.

Професор кафедри прикладної математики
та інформаційних технологій
Одеського національного політехнічного університету
д. т. н., проф.



Крилов В.М.

Підпис професора кафедри прикладної математики
та інформаційних технологій
Крилова В.М. засвідчую:

