Голові разової спеціалізованої вченої ради
Державного університету
«Київський авіаційний інститут»
доктору технічних наук, професору
Гнатюку Сергію Олександровичу

ВІДГУК

офіційного опонента, доктора технічних наук, професора
професора кафедри безпеки інформації та телекомунікацій
Національного технічного університету «Дніпровська політехніка»
Корченко Анни Олександрівни
на дисертацію Петляк Наталії Сергіївни
«Моделі та методи виявлення аномального трафіку в інформаційно-комунікаційних системах», подану на здобуття ступеня доктора філософії за спеціальністю 125 – Кібербезпека
галузі знань 12 – Інформаційні технології

1.Актуальність теми дисертації

Дисертаційна робота Петляк Наталії Сергіївни присвячена актуальній у контексті сучасних кіберзагроз темі виявлення аномального трафіку в інформаційно-комунікаційних системах. У сучасному цифровому середовищі, де щодня зростає кількість і складність кібератак, виникає потреба у вдосконаленні підходів до аналізу мережевої активності, зокрема в частині виявлення відхилень від типових характеристик трафіку. Забезпечення безпеки інформаційного простору, особливо у вихідному сегменті трафіку, де нерідко приховуються ознаки внутрішніх загроз, є ключовим чинником у підтримці сталого функціонування ІКС.

Необхідність дослідження зумовлена обмеженнями традиційних сигнатурних систем, які виявляють лише відомі атаки, залишаючи без уваги нові, модифіковані чи розподілені загрози. Актуальність теми підтверджується статистикою кібератак останніх років, що засвідчує стрімке зростання кількості інцидентів, пов'язаних із несанкціонованим доступом, витоками даних, а також використанням корпоративних мереж для запуску DDoS-атак.

Дисертаційна робота спрямована на розвиток теоретичних засад і практичних методів виявлення аномалій у мережевому трафіку з урахуванням поведінкових характеристик користувачів і зловмисників, що забезпечує підвищення точності, адаптивності та достовірності системи кіберзахисту. Результати дослідження мають важливе прикладне значення для побудови нових архітектур засобів виявлення вторгнень, що функціонують у реальному часі.

2.Основний зміст роботи

У вступі обґрунтовано актуальність дисертаційного дослідження, визначено мету, об'єкт і предмет роботи, сформульовано основні наукові завдання, викладено наукову новизну та практичну значимість отриманих результатів. Визначено особистий внесок здобувачки, подано відомості про

апробацію результатів на конференціях, наукові публікації та структуру роботи.

У першому розділі дисертації здійснено аналіз сучасного стану проблеми виявлення аномального трафіку в інформаційно-комунікаційних системах. Оцінено існуючі методи та моделі виявлення аномалій, їх переваги й недоліки, зокрема в умовах динамічного трафіку та новітніх загроз. Визначено потребу в орієнтації дослідження на аналіз саме вихідного трафіку, який часто не охоплюється стандартними засобами моніторингу, але може містити важливу інформацію щодо потенційної зловмисної активності. Обґрунтовано напрями вдосконалення підходів на основі гібридизації моделей та нечіткої логіки.

У другому розділі представлено моделі поведінки типового користувача та потенційного зловмисника в мережі, а також вдосконалено моделі класифікації трафіку, включаючи модель сигнатури пакету, модель класифікації за ознаками і на основі самоподібності. Запропоновано використання нечіткої класифікації для врахування невизначеності та неповноти вхідних даних, що підвищує чутливість до відхилень у поведінці трафіку.

У третьому розділі розроблено та вдосконалено методи виявлення аномального трафіку на основі описаних моделей. Зокрема, запропоновано гібридний метод, що поєднує класифікацію за ознаками, аналіз самоподібності та нечіткий висновок, що дозволило зменшити хибні спрацювання та підвищити точність виявлення. Проведено експериментальну перевірку ефективності методів.

У четвертому розділі реалізовано структурну модель системи виявлення аномального трафіку з використанням розробленого гібридного методу. Описано архітектуру системи, модулі класифікації, логування та обробки трафіку. Результати експериментів у тестовому середовищі підтвердили підвищену достовірність і адаптивність системи при змінних умовах мережі.

Основні висновки містять отримані у роботі наукові і практичні результати та відповідають заявленій меті і завданням дослідження.

3.Наукова новизна дисертаційної роботи

– *вдосконалено* модель сигнатури пакету для пошуку аномального трафіку, що за рахунок виключення з параметрів сигнатури розміру заголовка, контрольної суми заголовку, корисного розміру пакета, мітки потоку, пріоритету пакету, контрольної суми пакету за принципом Парето, забезпечило зменшення часу аналізу трафіку.

– *вдосконалено* модель процесу нечіткого виявлення аномального трафіку, в якій за рахунок використання експертного підходу сформована множина правил та набір відповідних лінгвістичних змінних, що дозволило розробити нові підходи до виявлення аномального трафіку в інформаційно-комунікаційних системах.

– *вперше* розроблено гібридний метод виявлення аномального трафіку в інформаційно-комунікаційних системах в якому за рахунок інтеграції методу класифікації трафіку за ознаками, методу самоподібності та розробленої моделі процесу нечіткого виявлення дозволило динамічно формувати множини сигнатур при класифікації трафіку за ознаками та підвищити показники виявлення аномального трафіку.

– *вдосконалено* структурну модель системи виявлення аномального трафіку в інформаційно-комунікаційних системах, що за рахунок інтегрування розробленого гібридного методу виявлення аномального трафіку в інформаційно-комунікаційних системах та динамічного варіювання множиною дозволених та заборонених з'єднань у режимі реального часу дозволило зменшити навантаження на процесор.

4.Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації, та їх достовірність

Результати дисертаційної роботи є науково обґрунтованими та узгоджуються з чинними теоріями інформаційної безпеки, не суперечать фізичним законам і загальноприйнятим уявленням про функціонування інформаційно-комунікаційних систем. У процесі дослідження коректно використано сучасні методи теорії нечітких множин, методи класифікації, аналізу самоподібності, а також методи гібридного моделювання. До розв'язання поставлених задач залучено підходи системного аналізу, експертних оцінок і статистичного моделювання. Достовірність отриманих результатів підтверджено результатами численних експериментів у тестовому середовищі, що демонструють високу точність і адаптивність запропонованих методів до реальних умов функціонування мережі.

5.Практичне значення отриманих результатів

1. Одержані в дисертаційній роботі результати стали підґрунтям для забезпечення зменшення обсягів аномального трафіку в інформаційно-комунікаційні системі.

2. Розроблено алгоритмічне забезпечення системи виявлення аномального трафіку в інформаційно-комунікаційних системах, що реалізує гібридний метод, його складові метод класифікації трафіку за ознаками, метод самоподібності, нечіткий метод та моделі, що в них використовуються.

3. На основі алгоритму розроблено програмний застосунок, що дозволяє проводити аналіз трафіку в інформаційно-комунікаційних системах.

4. Можливість практичного використання розробленого програмного застосунку сумісно з маршрутизаторами в інформаційно-комунікаційній системі.

5. Результати дисертаційної роботи апробовано і використано у ТОВ «X-CITY» (акт впровадження від 10.04.2025р) та у навчальному процесі кафедри кібербезпеки Хмельницького національного університету (акт впровадження від 25.03.2025р.).

6.Апробація результатів дисертації

Результати дисертації доповідались та обговорювались на конференціях, серед яких: II студентська науково-технічна конференція «Інформаційна, функційна та кібербезпека» (СКІФіК-2022) (Харків, 2022), The International Workshop on Intelligent Information Technologies & Systems of Information Security (Хмельницький, 2022), VI Міжнародна науково-практична конференція «Інформаційна безпека та комп'ютерні технології» (Кропивницький, 2023), XII

Міжнародна науково-технічна конференція ITSec: Безпека інформаційних технологій (Ужгород, 2023), IX Міжнародна науково-практична конференція Захист інформації і безпека інформаційних систем (Львів, 2023), 13th International Conference on Dependable Systems, Services and Technologies (Athens, 2023), XIII Міжнародна науково-технічна конференція ITSec: Безпека інформаційних технологій (Львів, 2024), 4the International Workshop on Intelligent Information Technologies & Systems of Information Security (Хмельницький, 2024), 1st International Workshop on Advanced Applied Information Technologies (Khmelnytskyi, 2024), 1st International Workshop on Intelligent and CyberPhysical Systems (Khmelnytskyi, 2024), 2nd International Workshop on Computer Information Technologies in Industry 4.0 (Ternopil, 2024).

7.Публікації здобувача

За матеріалами дисертаційних досліджень опубліковано 17 наукових робіт, у тому числі: 6 наукових статей – у наукових фахових виданнях України; 11 тез і матеріалів доповідей на міжнародних і науково-практичних конференціях, з них 5 – у рецензованому виданні, що входить до бази даних Scopus, 1 – у рецензованому виданні, що входить до бази даних IEEE.

8.Зауваження до дисертаційної роботи

1. В першій науковій новизні зазначений кількісний ефект щодо забезпечення зменшення часу аналізу трафіку, але у висновках до роботи не представлено конкретних числових значень.

2. У другому пункті наукової новизни зазначається, що запропоновано вдосконалення моделі процесу нечіткого виявлення аномального трафіку, яка ґрунтується на експертному підходу на базі якого сформована множина правил та набір відповідних лінгвістичних змінних, але в розділі 2.6 де здійснюється розробка такої моделі чітко не формалізовані зазначені базові складові.

3. У вступі на сторінці 24 в практичній цінності зазначено, що запропоновано удосконалення методу та розроблено гібридний метод, що більше відноситься не до практичної цінності, а до наукової новизни, хоча в анотації на сторінці 7 чітко визначена практична цінність.

4. В роботі є не зовсім коректне використання певних змінних, наприклад, е формулі 2.1 маленькою літерою d позначено багатокомпонентний кортеж, а в формулі 2.3 d використовується в якості індекса величини N, що позначає кількість елементів множини вхідних сигнатур (N_d).

5. В роботі при оцінці самоподібності трафіку не обґрунтовано тривалості часових інтервалів t1-t2 та t2-t3.

6. У формулі 2.16 не зазначено, що кількість сигнатур n не може дорівнювати 0, оскільки тоді формула 2.18 втратить практичний сенс.

7. В роботі використовується термін аномалія, однак відсутнє визначення, що саме в цій роботі розуміється під терміном аномалія.

9.Висновок

Розглядаючи роботу в цілому та незважаючи на вказані зауваження, вважаю, що загальна оцінка роботи є позитивною. Дисертаційна робота Петляк

Наталії Сергіївни «Моделі та методи виявлення аномального трафіку в інформаційно-комунікаційних системах» є завершеною науковою працею, яка виконана здобувачем самостійно і відповідає принципам академічної доброчесності.

У роботі отримано нові науково-технічні результати щодо розробки моделей та методів виявлення аномального трафіку в інформаційно-комунікаційних системах. Проведено аналіз сучасного стану проблеми кіберзахисту, обґрунтовано необхідність дослідження вихідного трафіку, який залишається поза увагою традиційних систем виявлення загроз.

Запропоновано гібридний метод виявлення аномалій, що поєднує класифікацію за ознаками, самоподібністю та методи нечіткого аналізу. Розроблено структурну модель системи виявлення аномального трафіку, а також реалізовано алгоритмічне та програмне забезпечення для її впровадження в реальні умови. Верифікація результатів підтвердила ефективність і практичну значущість запропонованих рішень. Результати апробовано у практичній діяльності та навчальному процесі.

Вважаю, що за актуальністю вибраної теми, обсягом і рівнем виконаних теоретичних і експериментальних досліджень, достовірністю і обґрунтованістю висновків, новизною досліджень, значенням отриманих результатів для науки і практики дисертаційна робота відповідає вимогам до дисертаційних досліджень на здобуття ступеня доктора філософії, визначеним Постановою Кабінету Міністрів України №44 від 12.01.2022 «Про затвердження Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу освіти, наукової установи про присудження ступеня доктора філософії».

Дисертаційна робота може бути представлена до офіційного захисту у разовій спеціалізованій вченій раді, а її автор, Петляк Наталія Сергіївна, заслуговує на присудження ступеня доктора філософії за спеціальністю 125 – Кібербезпека галузі знань 12 – Інформаційні технології.

ОФІЦІЙНИЙ ОПОНЕНТ:
доктор технічних наук, професор
професор кафедри безпеки
інформації та телекомунікацій
Національного технічного університету
«Дніпровська політехніка» Анна КОРЧЕНКО

14.07.2025

Підпис Корченко А. О. засвідчую

Вчений секретар Вченої ради
Національного технічного університету
«Дніпровська політехніка»,
канд. пед. наук, доцент Таісія КАЛЮЖНА