РЕЦЕНЗІЯ

рецензента, кандидата технічних наук,
старшого наукового співробітника Ткачова Андрія Михайловича
на дисертаційну роботу **Толкачова Максима Юрійовича**
“Моделювання безпеки інтернет-трафіку як семіотичної системи”,
подану на здобуття наукового ступеня доктора філософії
за спеціальністю 125 – Кібербезпека та захист інформації

Актуальність теми. Актуальність теми дисертаційної роботи "Моделювання безпеки інтернет-трафіку як семіотичної системи" зумовлена глибокими трансформаціями в галузі кібербезпеки, які пов'язані з швидким розвитком інформаційних технологій, зростанням кількості цифрових загроз, а також ускладненням структури сучасного інтернет-трафіку. У сучасному цифровому суспільстві інтернет-трафік є не лише технічним потоком даних, а й носієм складного інформаційного змісту, який відображає соціальні, поведінкові та контекстуальні характеристики взаємодії користувачів у кіберпросторі. Відповідно, класичні технічні засоби захисту, які базуються переважно на сигнатурному аналізі та статичних правилах, стають дедалі менш ефективними у протидії складним загрозам, зокрема цільовим атакам, що використовують методи соціальної інженерії та штучного інтелекту.

Одним із важливих чинників актуальності теми є стрімке розширення кіберфізичного простору, де інтернет-трафік виступає ключовим каналом передачі даних між компонентами соціокіберфізичних систем. У таких умовах рівень безпеки трафіку визначає загальну стійкість цифрової інфраструктури держави, включаючи критичні об'єкти інфраструктури, банківські системи, системи електронного врядування та об'єкти промислового інтернету речей (IIoT). Тому наукові дослідження, спрямовані на вдосконалення методів аналізу, виявлення та протидії кіберзагрозам у трафіку з урахуванням його змістової природи, є надзвичайно важливими.

В умовах гібридних загроз та інформаційних впливів, які часто мають перцептивний характер, виникає потреба у багаторівневому підході до аналізу інтернет-трафіку. Семіотична модель, яка враховує синтаксичний, семантичний, прагматичний і соціальний рівні інформації, дозволяє не тільки ідентифікувати загрозу на ранній стадії, а й оцінити потенційний вплив переданої інформації на поведінку користувачів та функціонування інформаційної системи в цілому. Таким чином, семіотичний підхід дозволяє розширити можливості систем захисту інформації за межі технічного аналізу, інтегруючи в них інструменти соціального, поведінкового та контекстуального моделювання.

Не менш важливою є актуальність теми в контексті реалізації Стратегії кібербезпеки України на 2021–2025 роки, де підкреслюється необхідність зміцнення національної системи кіберзахисту через розвиток інноваційних технологій, зокрема засобів моніторингу, аналізу ризиків та попередження атак. Запропоноване в дисертації дослідження безпосередньо відповідає цим цілям, оскільки передбачає створення інтегрованої моделі захисту, яка ґрунтується на новітніх підходах семіотичного аналізу та концепції нульової довіри.

Окремо слід зазначити, що вітчизняна та зарубіжна наукова спільнота лише нещодавно почала активно звертати увагу на семіотичні аспекти аналізу кіберзагроз. У зв'язку з цим, представлене дослідження заповнює існуючу наукову прогалину, пропонуючи інноваційний підхід до класифікації та ідентифікації інформаційних потоків у мережі. Вперше було запропоновано алгоритм аналізу інформаційного ресурсу на основі багаторівневої структури, що враховує семіотичні властивості трафіку та дозволяє ефективно сегментувати потоки залежно від рівня загрози, змісту та контексту.

Отже, ступінь актуальності теми дисертаційної роботи визначається низкою факторів: трансформацією інтернет-трафіку в складну інформаційно-соціальну систему; зростанням кіберзагроз, які виходять за межі технічного аналізу; необхідністю впровадження новітніх моделей кіберзахисту; а також державною політикою у сфері цифрової безпеки. Результати дисертаційної роботи мають не лише теоретичне, а й значне практичне значення, оскільки

можуть бути інтегровані у реальні системи захисту як у державному, так і в корпоративному секторах.

Таким чином, дане дослідження робить вагомий внесок у розвиток сучасних інформаційних технологій та є актуальним для широкого кола фахівців, включаючи розробників програмного забезпечення, спеціалістів з інформаційної безпеки, аналітиків, науковців і представників державних органів, відповідальних за стратегічне планування та захист інформаційного простору країни. Тому тема дисертаційної роботи Толкачова Максима Юрійовича "Моделювання безпеки інтернет-трафіку як семіотичної системи" є актуальною з наукової та практичної точок зору та має важливу технічну значущість.

Зв'язок роботи з науковими програмами, планами, темами. Тематика дисертаційної роботи відповідає пріоритетним напрямам розвитку науки і техніки в Україні з розділу "Інформаційні та комунікаційні технології". Отримані результати дисертаційної роботи є частинами наукових досліджень кафедри кібербезпеки НТУ "Харківський політехнічний інститут" у межах ініціативної науково-дослідної роботи "Моделювання соціо-кіберфізичних систем" (ДР № 0123U101018, 2023).

Наукова новизна одержаних результатів. У дисертаційній роботі Толкачова М.Ю. отримано такі науково обґрунтовані результати:

– Вперше обґрунтовано використання семіотичного аналізу як основи для формування багаторівневої системи захисту, яка дозволяє виявляти не лише технічні загрози, а й змістовно-соціальні аномалії в інформаційному потоці.

– Розроблено універсальну модель багатошарового аналізу трафіку. Модель враховує не лише фізичні й протокольні параметри трафіку, а й його семантику, контекст використання та вплив на поведінку користувачів, що дозволяє забезпечити адаптивний захист в умовах постійно змінюваного кіберпростору.

– Удосконалено механізми маркування та сегментації інформаційних потоків. Запропоновано дворівневу технологію маркування трафіку (макро- та

мікросегментація), яка реалізується динамічно, з урахуванням семіотичних ознак даних, що значно підвищує точність розмежування доступу та знижує ймовірність компрометації.

– Запропоновано нову систему оцінювання рівня загроз, яка враховує взаємозв'язки між структурними, смисловими та поведінковими параметрами трафіку, що дозволяє більш об'єктивно визначати потенційну небезпеку інциденту.

Вважаю, що робота дисертанта є внеском у розробку моделей безпеки інтернет-трафіку у кібефізичному просторі на основі багаторівневої семіотичної моделі, що забезпечує підвищення рівня безпеки систем захисту інформації.

Наукова та практична цінність одержаних результатів. Наукова цінність дисертаційної роботи полягає у створенні концептуально нової моделі забезпечення безпеки інтернет-трафіку на основі семіотичного підходу. Запропоноване моделювання враховує не лише технічні параметри трафіку, а й його зміст, контекст і соціальний вплив, що дозволяє досліджувати кіберпростір як складну інформаційну систему з багаторівневою структурою. Вперше розроблено алгоритм, який поєднує семантичний, синтаксичний і прагматичний аналіз у процесі виявлення загроз, що забезпечує підвищення точності та адаптивності систем захисту у порівнянні з традиційними методами.

Практична цінність полягає в можливості інтеграції отриманих результатів у реальні системи кіберзахисту різного рівня складності – від корпоративних мереж до об'єктів критичної інфраструктури.

Результати дослідження були впроваджені у:

– мережевій підсистемі захисту Інтернет-банкінгу "ELPay" товариства з обмеженою відповідальністю "Сайфер ІТ" (акт від 19.03.2025 року);

– навчальний процес НТУ "ХПІ" при викладанні курсів "Безпека хмарних технологій", "Основи смарт-контрактів" та "Blockchain: основи та приклади застосування" для вітчизняних та іноземних студентів ОПП "Кібербезпека" першого (бакалаврського) та другого (магістерського) рівнів вищої освіти (акт від 22.05.2025 року),

– діяльності товариства з обмеженою відповідальністю "Мікрокрипт Текнолоджис" (акт від 23.04.2025 року).

Повнота викладення матеріалів дисертації в наукових працях, які опубліковані автором. Основні положення та результати дисертаційного дослідження пройшли апробацію та були опубліковані у наукових журналах України, що входять до переліку фахових видань, а також у науково-технічних журналах, індексованих у міжнародних наукометричних базах, що відповідає встановленим вимогам для дисертаційних робіт на здобуття наукового ступеня доктора філософії.

За результатами дослідження дисертаційної роботи опубліковано 13 наукових праць, серед яких: одна одноосібна стаття у науковому фаховому виданні України категорії "Б", 2 статті – у наукових фахових виданнях України категорії "Б", 1 стаття – у закордонному періодичному виданні, 2 статті – у наукових фахових виданнях, що входять до наукометричної бази Scopus, 4 публікації у збірниках матеріалів та тез конференцій, 2 деклараційні патенти України на винахід, 1 монографія (видання, що включено до наукометричної бази Scopus). Участь здобувача у роботах, що опубліковані у співавторстві, зазначена у дисертаційній роботі. Зазначене вище дозволяє стверджувати, що представлена дисертаційна робота є самостійним, завершеним науковим дослідженням, результати якого мають значення для сфери кібербезпеки.

Аналіз змісту дисертації. Ступінь обґрунтованості наукових положень, висновків та рекомендацій, сформульованих у дисертаційній роботі. Побудова дисертації відповідає прийнятим для наукового дослідження нормам. Усі положення, винесені на захист, висвітлені в тексті дисертації. Зміст дисертаційної роботи відповідає її назві.

Дисертація написана грамотною науковою мовою та оформлена відповідно до існуючих нормативних документів, текст і графічний матеріал виконані акуратно з використанням комп'ютерної техніки.

Дисертаційна робота Толкачова М.Ю. має чітку структуру, що включає вступ, чотири розділи, висновки, список використаних джерел і додатки.

Перший розділ присвячений огляду існуючих методів захисту інтернет-трафіку та систем контролю доступу в інфокомунікаційних мережах. Проаналізовано типи кібератак на різні види трафіку та визначено вразливі сегменти мережевої інфраструктури. Обґрунтовано необхідність нових підходів до безпеки, які враховують не лише технічні, а й соціальні та перцептивні фактори.

У *другому розділі* представлено модель кіберпростору як семіотичної системи, що охоплює синтаксичний, семантичний, прагматичний і соціальний рівні інформації. Розглянуто структуру інтернет-комунікацій та запропоновано ієрархію надійності в цифровому середовищі. Показано, як семіотичний підхід дозволяє підвищити ефективність політик безпеки через глибше розуміння змісту трафіку.

Третій розділ містить розробку семіотичної моделі динамічного аналізу і маркування трафіку, що дозволяє здійснювати адаптивний контроль доступу. Запропоновано методи сегментації даних з використанням моделі зрілості Zero Trust. Обґрунтовано застосування семіотичного підходу для побудови захисних механізмів із урахуванням змішаного змісту інформаційних потоків.

Четвертий розділ присвячено моделюванню та експериментальній перевірці запропонованих моделей на основі реальних наборів даних CIC-IDS та NSL-KDD. Проаналізовано точність виявлення складних загроз і порівняно ефективність системи з існуючими рішеннями. Підтверджено доцільність впровадження семіотичного підходу для підвищення рівня кіберзахисту в різних мережевих середовищах.

Висновки, сформульовані у роботі, висвітлюють результати дослідження як вирішення висунутих в дисертації завдань. Висновки відповідають вимогам, які висуваються до результатів дисертаційного дослідження на здобуття наукового ступеня доктора філософії.

Список використаних джерел широко охоплює предметне поле дослідження, певною мірою відображає опрацювання автором значної кількості

джерел, пов'язаних з захистом інформації та інтелектуальними методами оцінки ефективності.

Додатки містять інформацію про практичне впровадження результатів дисертації, фрагменти кодів програм та список публікацій здобувача.

Достовірність отриманих результатів та висновків.

Грунтовний аналіз дисертаційної роботи свідчить, що її наукові положення, висновки та рекомендації є достатньо обґрунтованими, повними та аргументованими. Автор провів як теоретичні, так і емпіричні дослідження, використовуючи актуальні вітчизняні та міжнародні джерела. Достовірність висновків підтверджується застосуванням класичних і сучасних методів досліджень, логічним аналізом літератури, а також коректним формулюванням актуальних завдань.

Результати досліджень доповідалися на міжнародних науково-технічних конференціях і публікувалися у фахових виданнях. Узгодженість отриманих результатів, їх відповідність літературним даним і успішне впровадження підтверджують їх достовірність. У межах дисертаційного дослідження автор повністю реалізував поставлену мету і завдання, а логічні висновки до кожного пункту роботи дозволяють чітко зрозуміти основні етапи дослідження та практичну цінність отриманих результатів. Достовірність висновків підкріплюється комплексним підходом до вивчення визначеного об'єкта. Вищевикладене свідчить про обґрунтованість та достовірність наукових положень, висновків і рекомендацій, що викладено у дисертаційній роботі Толкачова Максима Юрійовича.

Оформлення дисертації, дотримання вимог академічної доброчесності та повнота викладення наукових положень та результатів в опублікованих працях. Дисертація виконана з дотриманням вимог академічної доброчесності, отримані результати дають підстави говорити про оригінальність роботи. У тексті містяться авторські ідеї, і не виявлено використання ідей інших науковців без посилання на їх роботи

Основні ідеї автора та результати дослідження викладено у шести статтях, а також дисертант активно приймав участь в науково-практичних конференціях, де була проведена апробація ідей, що викладено у дисертаційному дослідженні.

Недоліки та зауваження до дисертаційної роботи.

В процесі ознайомлення з роботою позитивне враження справило докладне обґрунтовування усіх висунутих у роботі положень, використання сучасних математичних методів.

Але при цьому виникли такі зауваження.

1. В п. 1.1.2 дисертаційної роботи не визначені спеціальні механізми, які забезпечують безпеку в постквантовий криптоперіод.

2. В дисертаційній роботі на рис. 2.1 наведений семіотичний трикутник, що ілюструє порівняння концепцій, але не зрозуміло яким чином визначаються окремо концепції Пірса, Бакленда, Хуанга.

3. На стор. 77 дисертаційної роботи наведені вагові показники вразливостей, але не зрозуміло яким чином вони визначені.

4. З дисертаційної роботи не зрозуміло яким чином архітектура управління безпекою трафіку (рис.3.8, стор. 93) впливає на запропоновану семіотичну модель безпеки.

5. В табл. 4.1 дисертаційної роботи (стор. 115) наведений аналіз кібербезпеки окремих власників мережі, в якому не зрозуміло яким чином визначений рівень захищеності мережі.

Проте наведені у результаті аналізу роботи зауваження не впливають на загальне позитивне враження від роботи, не зменшують її якості, а також наукової та практичної цінності. Вони не є визначальними і можуть бути враховані як напрямки подальших досліджень.

Висновки. Дисертаційна робота Толкачова Максима Юрійовича є завершеною науково-дослідною роботою, яка містить науково-обґрунтовані результати, має наукову новизну та дає перспективи подальших досліджень.

Тема дослідження відповідає галузі знань 12 – Інформаційні технології та спеціальності 125 – Кібербезпека та захист інформації.

За змістом, актуальністю, ступенем новизни, обґрунтованістю, науковою та практичною значимістю одержаних результатів дисертаційна робота "Моделювання безпеки інтернет-трафіку як семіотичної системи" відповідає вимогам п.п. 6, 7, 8, 9 "Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії", із змінами, внесеними згідно з Постановою Кабінету Міністрів України № 341 від 21.03.2022, затвердженого постановою Кабінету Міністрів України від 12 січня 2022 р. № 44, а її автор, Толкачов Максим Юрійович, заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 125 – Кібербезпека та захист інформації.

Рецензент – доцент кафедри кібербезпеки
Національного технічного університету
"Харківський політехнічний інститут"
кандидат технічних наук,
старший науковий співробітник Андрій ТКАЧОВ

Підпис Андрія Ткачова
ЗАСВІДЧУЮ:
ВЧЕНИЙ СЕКРЕТАР
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"
"29" 07 2025 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * Національний технічний університет "Харківський політехнічний інститут" * код 02071180 *