ВІДГУК

офіційного опонента доктора технічних наук, професорки,
завідувачки кафедри інформаційних технологій,
Одеського національного університету імені І. І. Мечнікова,
Казакової Надії Феліксівни
на дисертаційну роботу Толкачова Максима Юрійовича
“Моделювання безпеки інтернет-трафіку як семіотичної системи”,
поданої на здобуття наукового ступеня доктора філософії
за спеціальністю 125 – Кібербезпека та захист інформації

1. Актуальність теми дисертації

На сьогоднішній день забезпечення кібербезпеки є однією з найважливіших задач у сфері інформаційних технологій, що зумовлено активною цифровізацією державного управління, бізнесу та соціальної комунікації. Швидке зростання обсягів інтернет-трафіку та його складна структура, яка включає мультимедійні, текстові й інтерактивні дані, потребують застосування новітніх підходів до аналізу та захисту інформаційних потоків. Сучасні загрози, зокрема APT-атаки, кібершпигунство, соціотехнічні впливи, дезінформаційні кампанії та інструменти, що використовують штучний інтелект, виходять за межі традиційного сигнатурного або статичного аналізу. У зв’язку з цим семіотичний підхід, який враховує смислову природу даних та їхній контекст, постає як інноваційний інструмент підвищення ефективності кіберзахисту в кіберпростірі.

У дисертаційній роботі Толкачова Максима Юрійовича запропоновано нову концепцію безпеки інтернет-трафіку, засновану на багаторівневій семіотичній моделі, яка охоплює фізичний, синтаксичний, семантичний, прагматичний та соціальний рівні. У межах дослідження створено методологію

семіотичного аналізу інформаційного потоку для визначення рівнів ризику. Реалізовано методи цільової сегментації трафіку з використанням моделі CISA's Zero Trust Maturity Model. Запропоновано дворівневу технологію маркування даних, яка враховує змістове навантаження трафіку та дозволяє знижувати ймовірність компрометації ресурсів.

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.

2. Наукова новизна одержаних результатів.

В дисертаційній роботі 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.

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.

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.

Розроблено методику побудови індикаторів ризику на основі семіотичних факторів. 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.

3. Практичне значення отриманих результатів.

Практичне значення отриманих результатів полягає у можливості використання розробленої семіотичної моделі для підвищення ефективності систем моніторингу мережевого трафіку. Час обробки трафіку в експериментальному середовищі було знижено до 0,34 секунди на один запит, що свідчить про високу продуктивність моделі в режимі реального часу.

Практична цінність також полягає у використанні та впроваджені результатів досліджень:

– в експериментальну SIEM-підсистему (Security Information and Event Management) ТОВ "Мікрокрипт Технолоджис" (м. Харків) у вигляді програмної бібліотеки (акт від 23.04.2025 року);

– у мережевій підсистемі захисту Інтернет-банкінгу «ELPay». ТОВ "Сайфер ІТ" (м. Київ) (акт від 19.03.2025 року);

– у навчальний процес НТУ "ХПІ" (м. Харків) 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).

Мова та стиль викладення дисертації дозволяє зрозуміти суть розроблених наукових положень та одержаних практичних результатів. Дисертація відповідає вимогам, які висуваються до її оформлення, відповідно до "Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та

доктора наук у закладах вищої освіти (наукових установах)", що затверджений постановою Кабінету Міністрів України від 12 січня 2022 р. № 44 (зі змінами від 08 квітня 2025 року № 426), та "Вимог до оформлення дисертації" затверджених наказом Міністерства освіти і науки України від 12.01.2017 р. № 40. У цілому зміст дисертації викладено послідовно та логічно.

4. Ступінь обґрунтованості та достовірності наукових положень, висновків і рекомендацій, сформульованих у роботі.

Положення та висновки, сформульовані у дисертаційній роботі Толкачова Максима Юрійовича, мають належний рівень обґрунтованості як з наукової, так і з прикладної точки зору. Достовірність наукових результатів, висновків і рекомендацій підтверджено чисельними експериментами, математичним моделюванням, збіжністю результатів експериментів з відомими експериментальними даними інших академічних досліджень, відповідністю отриманих теоретичних результатів з результатами обчислювальних експериментів.

Усі дослідження проводилися із застосуванням засобів комп'ютерного моделювання та математичних методів, що забезпечило високу точність результатів. Обґрунтованість висунутих положень і практичних рекомендацій була підтверджена експериментально шляхом апробації запропонованих підходів, що свідчить про їх наукову і технічну доцільність.

5. Повнота оприлюднення результатів дисертаційної роботи

Основні результати дисертаційної роботи опубліковано в 13 наукових працях, із них 3 наукові статті у фахових виданнях України категорії "Б", 1 стаття у закордонному періодичному виданні, 2 статті опубліковано у наукових виданнях, які індексуються науково-метричною базою Scopus, 1 монографія (видання, що включено до наукометричної бази Scopus). 4 праці опубліковано у

матеріалах наукових конференцій та опубліковано 2 деклараційних патенти України на винахід.

Опубліковані матеріали повністю відображають зміст дисертації та відповідають вимогам пункту 8 Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого Постановою КМУ від 08 квітня 2025 року № 426.

6. Загальна характеристика структури та змісту дисертаційної роботи.

Дисертаційна робота Толкачова Максима Юрійовича складається зі вступу, чотирьох розділів, висновків, списку використаних джерел, 6 додатків.

У *вступі* дисертації викладено мотивацію обраного наукового напряму, обґрунтовано важливість теми в умовах зростаючої кількості кіберзагроз, визначено основну мету дослідження та окреслено перелік завдань, які необхідно вирішити для її досягнення. Також висвітлено наукову новизну, практичну цінність отриманих результатів, особистий внесок здобувача та наведено інформацію про апробацію й публікації за темою дисертації. Окрему увагу приділено зв’язку виконаного дослідження з державними і галузевими науковими програмами у сфері кібербезпеки.

Перший розділ присвячений аналізу існуючих підходів до захисту інтернет-трафіку, зокрема мережевих архітектур, методів реагування на кіберзагрози та класифікації кібератак. Розглянуто типи трафіку в інфокомунікаційних системах та визначено їхню вразливість до сучасних загроз, включаючи інформаційний вплив і маніпуляції. На основі аналізу обґрунтовано потребу в інтеграції інноваційних підходів, зокрема семіотичного аналізу, у системи безпеки.

У *другому розділі* подано концепцію кіберпростору як семіотичної системи, в якій відбувається взаємодія між користувачами, інформаційним контентом та інфраструктурою. Деталізовано структуру Інтернет-комунікацій, ієрархію рівнів інтерпретації трафіку та засоби семіотичного маркування для виявлення аномалій. Запропоновано модель безпеки, яка реалізує принцип нульової довіри, з використанням семантичних механізмів контролю доступу.

У *третьому розділі* здійснено розробку моделей, що враховують не лише технічні, а й смислові характеристики інформаційних потоків. Описано методи сегментації трафіку, дворівневе маркування даних, механізми динамічного контролю та оцінювання рівня захищеності на основі інтегрального показника. Представлено покращену семіотичну модель для адаптивного управління кібербезпекою.

Четвертий розділ присвячено експериментальному моделюванню на основі реальних даних (Cisco Talos, CIC-IDS, NSL-KDD), із використанням сучасних засобів програмного аналізу. Показано, як запропонований підхід дає змогу ефективно оцінити стан кіберзахисту, адаптувати політики безпеки та підвищити точність виявлення загроз. Наведено результати порівняльного аналізу та висновки щодо ефективності розроблених моделей.

Список використаних джерел із 110 найменувань досить повний і включає вітчизняні та зарубіжні публікації.

Анотація відображає основний зміст дисертації та достатньо повно розкриває наукові результати та практичну цінність роботи.

7. Зауваження по дисертаційній роботі

1. В дисертаційній роботі в табл. 1.5 (стор. 27) визначені типи кібератак за урахуванням видів трафіку, але не зрозуміло чому не визначений мовний трафік та які саме атаки є на цей тип.

2. В табл.1.6 дисертаційної роботи наведено порівняння різних підходів виявлення кібератак, але не зрозуміло, чому аналіз методів соціальної інженерії відноситься до методів виявлення, а також технологія блокчейн відноситься до питань кібербезпеки.

3. В дисертаційній роботі (рис. 2.2) наведений ланцюжок “антена-кіберпростір-соціальний вплив» інтегрований з рівнями семіотики, але не зрозуміло яким чином запропонована градація зліва на рисунку впливає на семіотичний аналіз запропонованої концепції.

4. На рис. 2.3 дисертаційної роботи (стор. 63) наведена інтегрована платформа безпеки, але не зрозуміло в чому саме полягає її інтеграція і який рівень захисту інформації вона забезпечує.

5. В дисертаційній роботі (рис. 2.8) наведена концепція побудови безпеки мережі за допомогою семіотичного підходу, але не зрозуміло в чому саме полягає ця концепція.

6. На стор. 77–79 дисертаційної роботи наведений математичний апарат оцінки різних аспектів безпеки, але не зрозуміло чому визначені тільки окремі рівні шестирівневої моделі та у чому полягає перевага запропонованої моделі до моделі ISO/OSI.

Вказані недоліки не впливають на загальну позитивну оцінку виконаної роботи. Дисертація є актуальною і має високу наукову цінність та практичну значущість.

8. Загальний висновок на дисертаційну роботу.

Дисертаційна робота Толкачова Максима Юрійовича “Моделювання безпеки інтернет-трафіку як семіотичної системи” за своїм змістом відповідає спеціальності 125 – Кібербезпека та захист інформації. Дисертація є завершеною науково-дослідною роботою, яка розв’язує важливе наукове завдання, яке полягає у розробці ефективних комплексних методів виявлення аномалій мережі

за інтегральними характеристиками трафіку на основі сучасної теоретичної бази, що визначило напрям дисертаційного дослідження.

Подана дисертаційна робота “Моделювання безпеки інтернет-трафіку як семіотичної системи” Толкачова Максима Юрійовича відповідає спеціальності 125 – Кібербезпека та захист інформації, відповідає вимогам до дисертацій на здобуття наукового ступеня доктора філософії, а саме вимогам пунктів 6, 7, 8 і 9 Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого Постановою КМУ від 12 січня 2022 р. № 44 (зі змінами від 08 квітня 2025 року № 426), а здобувач, Толкачов Максим Юрійович, заслуговує присудження наукового ступеня доктора філософії за спеціальністю 125 – Кібербезпека та захист інформації.

Офіційний опонент:

Завідувачка кафедри інформаційних технологій, Одеський національний університет імені І. І. Мечнікова, докторка технічних наук, професорка — Надія КАЗАКОВА

04.08.2025

Особистий підпис
Казакової Надії
ЗАСВІДЧУЮ
Ст. інспектор відділу кадрів
Любарська Г. В.

ВІДДІЛ КАДРІВ