РЕЦЕНЗІЯ

рецензента, доктора філософії, доцента,
завідувача кафедри програмної інженерії та інтелектуальних
технологій управління Коппа 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

Детальний аналіз дисертаційної роботи Толкачова М.Ю. на тему “Моделювання безпеки інтернет-трафіку як семіотичної системи”, що представлена для захисту на здобуття наукового ступеня доктора філософії у Національному технічному університеті «Харківський політехнічний інститут», дає змогу зробити комплексний висновок щодо її актуальності, ступеня обґрунтованості наукових положень, висновків, рекомендацій, достовірності та значущості отриманих результатів, наукової новизни, теоретичної та практичної цінності, надати загальну оцінку дисертації.

1. Ступінь актуальності теми дисертаційної роботи.

У сучасному цифровому світі стрімкий розвиток інформаційних технологій, зокрема глобалізація інтернет-інфраструктури та інтенсивне використання кіберфізичних систем, зумовили виникнення нових викликів у сфері забезпечення безпеки інформаційних ресурсів. Значне зростання обсягів інтернет-трафіку, його різнорідність та контентна насиченість сприяють не лише технічній, а й соціальній уразливості цифрового простору. Усе це створює умови, в яких традиційні методи виявлення та нейтралізації загроз виявляються недостатніми. У такому контексті тема дисертаційної роботи, присвячена моделюванню безпеки інтернет-трафіку як семіотичної системи, набуває особливої актуальності.

Однією з ключових проблем, що зумовлює актуальність дослідження, є відсутність інтегрованого підходу до захисту інформації, який одночасно

враховував би технічні характеристики трафіку, його змістову природу та соціальний контекст. Класичні системи захисту – антивіруси, брандмауери, IDS/IPS – переважно оперують сигнатурами або аномаліями на рівні мережевого протоколу, тоді як сучасні атаки дедалі частіше ґрунтуються на маніпуляції змістом інформації, поведінкових шаблонах користувачів та психологічному впливі. Саме ці обставини вимагають запровадження нового типу аналізу трафіку – семіотичного, який дозволяє врахувати множинні рівні сприйняття та інтерпретації даних.

Значна актуальність теми дисертації також підтверджується її відповідністю стратегічним цілям державної політики у сфері кібербезпеки. У Стратегії кібербезпеки України на 2021–2025 роки наголошується на необхідності модернізації національної системи кіберзахисту та розвитку інноваційних підходів до протидії складним інформаційним загрозам. З огляду на те, що кібербезпека охоплює не лише технічні аспекти, але й інформаційно-психологічні та соціальні, стає очевидним, що підхід, заснований на семіотичному аналізі інтернет-трафіку, є вкрай актуальним і перспективним для досягнення зазначених цілей.

Застосування семіотичного моделювання у сфері безпеки інтернет-трафіку відкриває можливості для створення адаптивних, контекстно-орієнтованих систем захисту, які здатні не лише виявляти загрози, але й аналізувати їхній зміст, мету та потенційний вплив. Семіотичний підхід дає змогу інтегрувати різні типи аналізу – синтаксичний, семантичний, прагматичний і соціальний – в єдину систему моніторингу, що особливо важливо у випадку змішаного контенту, властивого сучасному мережевому трафіку.

Наукова новизна роботи визначається тим, що вперше запропоновано комплексну модель кібербезпеки, яка базується на ідеї багаторівневої інтерпретації інформації, що циркулює в інтернет-трафіку. Актуальність цієї моделі підсилюється зростанням ролі соціокіберфізичних систем, де взаємодія між користувачами, пристроями та мережами формується не лише на основі технічних параметрів, а й через значення, які надаються інформації в конкретному контексті.

Враховуючи динамічність кіберзагроз та ускладнення механізмів атак, важливим є розроблення методів, здатних забезпечити гнучкість і пристосованість систем захисту. Саме таку можливість надає семіотичний підхід, що підтримує адаптивне маркування інформаційних потоків, сегментування трафіку та оцінювання рівнів ризику відповідно до змісту та контексту.

Отже, обрана тематика дисертаційного дослідження відповідає сучасному стану розвитку науки та технологій, вимогам інформаційного суспільства та завданням національної безпеки. Вона орієнтована на вирішення однієї з найбільш актуальних проблем – підвищення ефективності захисту інтернет-трафіку в умовах складного, багатофакторного кіберсередовища. Результати дослідження можуть бути практично використані в системах захисту корпоративних мереж, державних інституцій, критичної інфраструктури, а також у освітніх і наукових проєктах, що підтверджує високу прикладну значущість обраної теми.

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. Зв’язок роботи з науковими програмами, планами, темами.

Дисертаційне дослідження здійснювалося в межах наукової спеціальності 125 – Кібербезпека та захист інформації та виконувалося на базі кафедри кібербезпеки НТУ «ХПІ».

Результати, отримані в процесі виконання роботи, інтегровані в наукові дослідження, що здійснюються на кафедрі кібербезпеки НТУ «Харківський політехнічний інститут». Зокрема, положення дисертації є складовими ініціативної НДР «Моделювання соціо-кіберфізичних систем» (ДР № 0123U101018, 2023).

3. Наукова новизна одержаних результатів.

Наукова новизна одержаних результатів полягає в теоретичному осмисленні та впровадженні інноваційних рішень для створення багаторівневої семіотичної моделі захисту інтернет-трафіку в кібер-фізичному просторі, що забезпечує якісно новий рівень безпеки інформаційних систем. У дисертаційній роботі отримані такі основні науково обґрунтовані результати:

1. Вперше розроблено метод обчислення інтегрального показника загроз, що враховує зважене середнє шести семіотичних рівнів (фізичного, емпіричного, синтаксичного, семантичного, прагматичного та соціального), що дозволяє оцінювати змішані атаки з комплексними загрозами на відміну від класичних підходів.

2. Вперше побудовано семіотичну модель динамічного моніторингу та контролю інформаційних потоків у кіберпросторі, яка адаптивно змінює політики безпеки залежно від змісту та контексту трафіку.

3. Вперше покращено архітектурну модель корпоративної мережі з урахуванням CISA’s Zero Trust Maturity Model, що забезпечує дворівневе динамічне маркування даних та підвищує гнучкість і ефективність політик безпеки.

4. 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.

4. Наукова та практична цінність одержаних результатів.

Наукова та практична цінність одержаних результатів полягає в розробці інноваційного підходу до забезпечення кібербезпеки інтернет-трафіку на основі багаторівневої семіотичної моделі. Уперше було запропоновано розглядати трафік не лише як технічний потік даних, а як знакову структуру, що має синтаксичні, семантичні, прагматичні та соціальні рівні. Це дало змогу створити комплексний підхід до аналізу й маркування інформаційних потоків, здатний виявляти неочевидні загрози, у тому числі соціотехнічного характеру. Значущим науковим результатом є розробка інтегрального показника потенційних загроз, який враховує вплив різнорівневих характеристик контенту та дозволяє

оцінювати змішані атаки, що раніше важко піддавалися ідентифікації в межах класичних підходів.

Практична цінність дослідження полягає в тому, що розроблені моделі й алгоритми було реалізовано у вигляді програмних компонентів для динамічного моніторингу та захисту трафіку, протестованих на актуальних наборах даних CIC-IDS 2017/2018 і NSL-KDD 2022. Отримані результати демонструють підвищення точності виявлення загроз і скорочення часу реагування на інциденти, що робить запропоновані рішення ефективними для застосування в корпоративних мережах, фінансових установах, критичних інформаційних системах та органах державного управління. Розроблені технології можуть бути використані для вдосконалення існуючих систем класу SIEM, Zero Trust, SASE та інших, оскільки враховують як технічні, так і змістові аспекти безпеки. Таким чином, результати дисертаційного дослідження мають як важливе теоретичне значення для розвитку науки про кібербезпеку, так і прикладну цінність для широкого кола практичних завдань у сфері захисту інформації.

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).

5. Повнота викладення наукових і прикладних результатів дисертації в опублікованих працях та академічна доброчесність.

Основні ідеї здобувача та результати дослідження достатньо повно викладені у 1-й одноосібній статті у фаховому журналі категорії Б, у 2-х статтях із співавторами у журналах, що індексуються наукометричною базою Scopus, та у 2 статтях у фахових журналах категорії Б, у 1 статті у закордонному

періодичному виданні, що відповідає вимогам МОН України до опублікування результатів досліджень на здобуття наукового ступеня доктора філософії, 1 монографії (видання, що включено до наукометричної бази Scopus). Апробацію результати досліджень отримали на 4 міжнародних науково-технічних конференціях.

Дисертація виконана з дотриманням вимог 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. Зазначене вище дозволяє стверджувати, що представлена дисертаційна робота є самостійним, завершеним науковим дослідженням, результати якого мають значення для сфери кібербезпеки.

6. Ступінь обґрунтованості та достовірності наукових положень, висновків та рекомендацій, сформульованих у дисертаційній роботі.

Детальний аналіз дисертаційної роботи свідчить про те, що наукові положення, висновки та рекомендації, представлені в дослідженні, є достатньо обґрунтованими, повними та всебічно аргументованими. Для їх формулювання та підтвердження автор провів як теоретичні, так і емпіричні дослідження, включаючи експериментальні перевірки, використовуючи як вітчизняні, так і міжнародні спеціалізовані та актуальні джерела.

Достовірність отриманих результатів забезпечується застосуванням як класичних, так і сучасних методів дослідження, серед яких глибокий логічний аналіз літературних джерел, чітка постановка актуальних завдань та їх коректне вирішення. Результати теоретичних і експериментальних досліджень були представлені на науково-технічних конференціях та опубліковані у фахових наукових виданнях. Крім того, їх надійність підтверджується взаємоузгодженістю, відповідністю існуючим літературним даним і позитивними результатами практичного впровадження.

У ході дослідження автор повністю реалізував поставлену мету та завдання, визначені на початковому етапі роботи. До кожного розділу подано логічні висновки, що дозволяють чітко зрозуміти сутність дослідження та

практичну значущість отриманих результатів. Достовірність висновків також підтверджується комплексним підходом до аналізу досліджуваного об’єкта.

Таким чином, наведені факти свідчать про належний рівень обґрунтованості та достовірності наукових положень, висновків і рекомендацій, викладених у дисертаційній роботі Толкачова Максима Юрійовича.

7. Оцінка змісту дисертації, її завершеності й оформлення.

Побудова дисертації відповідає прийнятим для наукового дослідження нормам. Усі положення, винесені на захист, висвітлені в тексті дисертації. Зміст дисертаційної роботи відповідає її назві.

Дисертаційна робота Толкачова Максима Юрійовича написана грамотною науковою мовою та оформлена відповідно до існуючих нормативних документів, складається зі вступу, 4-х розділів, висновків, списку використаних джерел і 6-х додатків.

У *вступі* обґрунтовано актуальність теми дисертаційного дослідження, сформульовано мету дослідження та науково-прикладні завдання, необхідні для її досягнення, показано зв’язок дослідження з науковими програмами та темами, наведено наукову новизну отриманих результатів, їх практичну цінність та особистий внесок здобувача.

У *першому розділі* проаналізовано існуючі методи захисту інтернет-трафіку, зокрема інфраструктурні рішення та протокольні механізми. Досліджено особливості сучасних кібератак на різні типи трафіку, включаючи сигнальний, еластичний і потоковий. Проаналізовано проблеми виявлення атак у контексті зростаючої складності загроз, зокрема APT та соціотехнічних впливів. Обґрунтовано необхідність інтеграції нових підходів, які враховують семіотичну структуру трафіку й контекст передачі інформації.

У *другому розділі* представлено модель кіберпростору як семіотичної системи, що включає фізичний, синтаксичний, семантичний, прагматичний і соціальний рівні. Описано структуру інтернет-комунікацій як багаторівневої знакової системи з урахуванням контексту взаємодії користувачів. Запропоновано принципи маркування та сегментування інформаційного

контенту, що дозволяє формувати гнучкі політики безпеки. Розроблена ієрархія надійності трафіку як основа семіотичного аналізу у кіберпросторі.

У *третьому розділі* запропоновано семіотичну модель динамічного аналізу та маркування трафіку для контролю доступу. Розроблено методи макро- і мікросегментації інформаційних потоків відповідно до рівнів загрози. Описано формування інтегрального показника безпеки, який враховує зміст, контекст і соціальний вплив інформації. Представлено архітектуру захисної системи на основі моделі нульової довіри (ZTMM).

У *четвертому розділі* проведено моделювання ефективності запропонованих підходів на основі реальних датасетів CIC-IDS 2017/2018 та NSL-KDD 2022. Використано програмні скрипти на C# і Python для реалізації сценаріїв моделювання. Проведено порівняння результатів із традиційними системами захисту, зокрема Snort і Splunk ES. Показано переваги семіотичного аналізу щодо точності виявлення загроз і часу реагування.

Усі нові наукові положення, висновки та рекомендації, що виносяться на захист, є результатом самостійної роботи автора, пройшли апробацію та були опубліковані.

Анотація дисертації відображає її основний зміст, розкриває ключові наукові результати та підтверджує практичну значущість проведеного дослідження.

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, інтелектуальними методами та метриками оцінки їх ефективності.

Додатки містять додаткову інформацію про публікації здобувача та практичне впровадження результатів дисертації.

Дисертація виконана з дотримання 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.

8. Зауваження до дисертаційної роботи

В процесі ознайомлення з роботою позитивне враження справило докладне обґрунтовування усіх висунутих у роботі положень, використання сучасних математичних методів. Оцінка наукової роботи є позитивною, однак необхідно звернути увагу на наступні зауваження:

1. В п. 1.1 дисертаційної роботи наведений сучасний стан та тенденції розвитку методів захисту інформаційних ресурсів, але не зрозуміло чому під час розгляду основних загроз безпеки (таблиця 1.3) не визначені цільові атаки, які мають можливість комплексування з методами соціальної інженерії.

2. В табл. 2.1 дисертаційної роботи (стор.56) не зрозуміло, яким чином наведені в таблиці якості впливають на семіотичний аналіз Інтернет комунікацій.

3. На рис. 3.1 дисертаційної роботи наведені семіотичні рівні та ієрархія дані-інформація-знання, але не зрозуміло на якому етапі враховується семіотична модель і які рівні семіотики наведені на рисунку.

4. На рис. 3.5 наведений сценарій аналізу інформаційних потоків та маркування рівнів доступу у кіберпросторі, але не зрозуміло яким чином це впливає на рівень безпеки в рамках запропонованого підходу.

5. В табл. 4.3 дисертаційної роботи (стор. 122) визначені вихідні параметри для моделювання, але не зрозуміло, яким чином визначений рівень захищеності.

Проте наведені у результаті аналізу роботи зауваження не носять принципового характеру та жодним чином не знижують позитивне враження від роботи та її наукову та практичну цінність.

9. Відповідність дисертації встановленим вимогам і загальні 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 № 426 від 08.04.2025, затвердженого постановою Кабінету Міністрів України від 12 січня 2022 р. № 44, та вимогам до оформлення дисертації МОН України від 12.01.2017 № 40, а її автор, Толкачов Максим Юрійович, заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 125 – Кібербезпека та захист інформації.

Рецензент – Завідувач кафедри програмної
інженерії та інтелектуальних технологій
управління
Національного технічного університету
«Харківський політехнічний інститут»,
доктор філософії, доцент Андрій КОПП

Підпис
ЗАСВІДЧУЮ:
ВЧЕНИЙ СЕКРЕТАР
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"
"20" 07 2025

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