ВІДГУК

офіційного опонента доктора технічних наук, професора,
завідувача кафедри кібербезпеки та програмного забезпечення,
Центральноукраїнського національного технічного університету,
Смірнова Олексія Анатолійовича
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

Актуальність теми дисертаційної роботи обумовлена низкою сучасних викликів у сфері кібербезпеки. По-перше, стрімке впровадження інформаційно-комунікаційних технологій в Україні спричинило значне розширення обсягів та різноманітності інтернет-трафіку, що потребує нових підходів до його захисту. По-друге, зростання складності кіберзагроз, серед яких APT-атаки, соціотехнічні маніпуляції та використання штучного інтелекту, показало недостатність класичних сигнатурних і статичних методів аналізу трафіку. У цьому контексті семіотичний підхід, який передбачає аналіз трафіку на синтаксичному, семантичному, прагматичному та соціальному рівнях, відкриває можливості для більш гнучких і адаптивних систем захисту.

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.

Тому дисертаційна робота Толкачова Максима Юрійовича "Моделювання безпеки інтернет-трафіку як семіотичної системи", що спрямована на вирішення наукового завдання з розробки моделей безпеки інтернет-трафіку у

кібефізичному просторі на основі багаторівневої семіотичної моделі, є актуальною.

2. Наукова новизна одержаних результатів.

В дисертаційній роботі *вперше* розроблений метод обчислення інтегрального показника загроз, який 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. *Запропоновано* новий алгоритм аналізу трафіку, який поєднує синтаксичний, кореляційний, семантичний і прагматичний аналіз із маркуванням рівнів доступу, що суттєво знижує ентропію даних і підвищує точність виявлення інцидентів. *Вперше* побудовано семіотичну модель динамічного моніторингу та контролю інформаційних потоків у кіберпросторі, яка адаптивно змінює політики безпеки залежно від змісту та контексту трафіку.

3. Практичне значення отриманих результатів полягає у можливості використання розробленої семіотичної моделі мережевого трафіку, яка реалізована у вигляді програмного модуля на мові Python та апробована на основі даних з ресурсу Kaggle. Застосування цієї моделі дозволяє досягти точності класифікації трафіку до 94,2% при використанні модифікованого наївного баєсівського класифікатора, що підтверджено в ході експериментальних досліджень. Алгоритм здатен виявляти вторгнення типу DoS, Probe, R2L та U2R у вхідному трафіку за допомогою аналізу семіотичних ознак, що значно підвищує ефективність виявлення атак порівняно з класичними методами.

Практична цінність полягає в можливості інтеграції отриманих результатів у реальні системи кіберзахисту різного рівня складності.

Результати дослідження були впроваджені у:

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

– освітній 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);

– діяльності товариства з обмеженою відповідальністю "Мікрокрипт Текнолоджис" (акт від 23.04.2025 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, наведені в дисертаційній роботі Толкачова Максима Юрійовича, в достатній мірі обґрунтовані як з наукового, так і з технічного поглядів. Обґрунтованість отриманих у роботі наукових положень, висновків і рекомендацій базується на використанні математичного апарату методів аналітичного моделювання та нечіткої логіки. Наукові положення, висновки та рекомендації, сформульовані в дисертаційній роботі, базуються на

системному аналізі, математичному моделюванні та емпіричних даних, отриманих у процесі моделювання на актуальних датасетах. Запропоновані автором моделі проходили верифікацію на практичних прикладах, що свідчить про належний рівень достовірності результатів. Використання комплексного підходу, що включає семіотичний аналіз, дозволяє забезпечити логічну послідовність у формуванні висновків. Рекомендації щодо впровадження розроблених методів мають практичну орієнтацію та підтверджені апробацією в реальних інформаційних системах.

Дослідження виконані з використанням математичного апарату та сучасного комп'ютерного моделювання. Результати перевірені шляхом проведення практичних експериментів, що підтверджує обґрунтованість наукових положень, висновків і рекомендацій, сформульованих в дисертаційній роботі.

5. Повнота оприлюднення результатів дисертаційної роботи

Основні результати дисертації викладено в 13 наукових публікаціях: з них 2 статті у наукових фахових виданнях, що входять до наукометричної бази Scopus, а також 1 монографія (видання, що включено до наукометричної бази Scopus). 3 статті опубліковано у фахових виданнях України категорії «Б», 1 – у закордонному журналі. Крім того, 4 доповіді представлені в матеріалах наукових конференцій, отримано 2 деклараційні 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 12 січня 2022 р. № 44 (зі змінами від 08 квітня 2025 року № 426).

6. Загальна характеристика структури та змісту дисертаційної роботи.

Дисертаційна робота викладена на 201 сторінці та складається з анотації, змісту, списку скорочень, вступу, чотирьох основних розділів, в яких міститься 29 рисунків та 19 таблиць, списку використаних джерел з 110 найменувань, а також 6 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* здійснено огляд 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* запропонована модель семіотичної системи кіберпростору, яка враховує взаємодію між користувачами, контентом та мережевою інфраструктурою. Проаналізовано структуру Інтернет-комунікацій та визначено основні елементи їх семіотичної природи, включаючи синтаксичний, семантичний і прагматичний рівні. Розглянуто застосування семіотичної моделі для оцінки кібербезпеки, що дозволяє виявляти та нейтралізувати потенційні загрози за рахунок аналізу інформаційного контенту та його впливу на безпеку мереж.

У *третьому розділі* розроблено семіотичну модель 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.

У *четвертому розділі* проведено моделювання оцінки рівня кібербезпеки власників мережі. Моделювання проведено на основі даних звіту Cisco Talos за 2023 р. Для проведення моделювання запропоновані програмні застосунки і скріпти на мові C# і Python 3.x з використанням бібліотек Pandas, NumPy, SciPy.

Запропонований метод захисту змішаного контенту інформації інтернет-трафіку на основі семіотичного аналізу, який інтегрує стратегію нульової довіри та сучасні аналітичні технології та дає оцінку якісних та кількісних характеристик системи. Для проведення моделювання запропонованого підходу використані набори даних CIC-IDS 2017/2018 та NSL-KDD 2022, які базуються на алгоритмах виявлення атак та аналізу поведінкових характеристик трафіку.

Загальні висновки дисертаційної роботи узгоджуються з метою і завданнями дослідження. Отримані результати характеризуються науковою новизною та практичною цінністю, обґрунтовані теоретично та підтверджені експериментальними дослідженнями.

В цілому, дисертація Толкачова Максима Юрійовича є завершеним і повним дослідженням, яке містить теоретичні розробки та відповідні їм експериментальні перевірки.

7. Зауваження по дисертаційній роботі

1. На рис. 1.1 дисертаційної роботи наведений взаємозв'язок між властивостями мережевої інфраструктури, типами трафіку та протоколами, але не зрозуміло чому в механізмах безпеки не визначені специфікації протоколів, а саме, TLS і SSL.

2. В дисертаційній роботі (рис. 1.3) наведені основні напрямки використання новітніх інформаційних технологій та мережі Інтернет з

терористичною метою, але не зрозуміло яким чином враховуються методи соціальної інженерії, а також OSINT розвідка.

3. В наведеному аналізу (стор.60–62) в дисертаційної роботи не зрозуміло, який саме підхід до стратегії захисту інформації в інфокомунікаційних системах є найкращим та чому.

4. На стор. 62–63 дисертаційної роботи наведена модель загроз, яка передбачає концептуальний підхід, але не зрозуміло чому при цьому враховується тільки «архітектура нульової довіри».

5. В дисертаційній роботі (рис. 3.2) наведений багаторівневий підхід побудови системи безпеки, але не зрозуміло які саме рівні при цьому використовуються і яким чином забезпечується безпека на кожному із рівнів.

6. На рис. 4.1 дисертаційної роботи наведена математична модель оцінки рівня кібербезпеки власників мережі, але не зрозуміло, яким чином та які суб'єкти інформаційно-комунікаційної інфраструктури враховані за формою власності та правовим статусом.

Слід зазначити, що визначені зауваження не знижують загальної позитивної оцінки дисертаційної роботи.

8. Загальний висновок на дисертаційну роботу.

На основі критичного вивчення дисертації та праць здобувача, які опубліковані за темою дисертації об'єктивно встановлено:

– дисертаційна робота Толкачова Максима Юрійовича "Моделювання безпеки інтернет-трафіку як семіотичної системи", відповідає вимогам 6, 7, 8, 9 "Порядку присудження ступеня доктора філософії та скасування рішення разової спеціальної вченої ради Закладу вищої освіти, наукової установи про присудження ступеня доктора філософії" від 12.01.2022 р. № 44 (зі змінами від 08 квітня 2025 року № 426) та вимогам до оформлення дисертації МОН України від 12.01.2017 № 40;

– використання чужих наукових результатів без посилань на авторів у дисертації не виявлено, що свідчить про особистий внесок здобувача в науку;

– дисертаційна робота Толкачова Максима Юрійовича є завершеною науковою працею, в якій отримані нові науково обґрунтовані результати;

– автор дисертаційної роботи Толкачов Максим Юрійович заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 125 – Кібербезпека та захист інформації.

Офіційний опонент

завідувач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнського національного технічного університету
доктор технічних наук, професор Олексій СМІРНОВ

Підпис професора Смірнова О.А. засвідчую:
Проректор з наукової роботи та міжнародних зв'язків
Центральноукраїнського національного технічного університету,
кандидат технічних наук, доцент Андрій ТИХИЙ
“ 28 ” липня 2025 року