Голові разової спеціалізованої вченої ради
Державного університету
інформаційно-комунікаційних технологій
професору кафедри управління кібербезпекою
та захистом інформації Навчально-наукового
інституту кібербезпеки та захисту інформації
САВЧЕНКУ Віталію Анатолійовичу

ВІДГУК

офіційного опонента

ЄВСЕЄВА Сергія Петровича

Національного технічного університету «Харківський політехнічний інститут»
завідувача кафедри кібербезпеки
на дисертаційну роботу Рижакова Миколи Миколайовича на тему:
«МЕТОДИ ТА МОДЕЛІ ВИЯВЛЕННЯ АНОМАЛІЙ МЕРЕЖЕВОГО ТРАФІКУ НА ОБ'ЄКТАХ КРИТИЧНИХ ІНФОРМАЦІЙНИХ ІНФРАСТРУКТУР»
подану на здобуття наукового ступеня доктора філософії
за спеціальністю 125 – «Кібербезпека та захист інформації»,
галузь знань 12 – «Інформаційні технології».

1 Актуальність теми дисертації

Сучасні критичні інформаційні інфраструктури (енергетика, транспорт, охорона здоров'я, фінансовий сектор) стрімко діджиталізуються та покладаються на мережеві сервіси, хмарні й периферійні платформи. На цьому тлі зростає спектр кіберзагроз, що проявляються як високої інтенсивності (об'ємні L3/L4-DDoS, L7-атаки на веб- і API-сервіси), так і низькоінтенсивні/довготривалі відхилення (повільне виснаження ресурсів, C2-beaconing, латеральні переміщення, ексфільтрація даних, зміни профілів протоколів у сегментах ICS/SCADA). Питання виявлення аномалій мережевого трафіку на об'єктах критичних інформаційних інфраструктур (КІІ) є одним із визначальних для забезпечення кіберстійкості та безперервності функціонування критичних сервісів. Для КІІ характерні жорсткі вимоги до надійності, передбачуваності роботи та швидкості реагування, тоді як мережеве середовище демонструє високу мінливість параметрів і поведінкових патернів.

Додаткові труднощі виникають через використання шифрування, розподілених архітектур, наявність легітимних пікових навантажень та регулярних змін конфігурацій, що ускладнює відокремлення «нормальних» коливань від проявів зловмисної активності або деградаційних процесів. У практичних контурах моніторингу важливо не лише фіксувати відхилення, а й швидко визначати їх інциденту значущість та пріоритет.

У цьому контексті актуальним є поєднання методів глибокого навчання, адаптивних механізмів порогування, семантичної атрибуції та оцінювання критичності подій, що й становить науково-прикладний зміст дисертаційної роботи.

2 Наукова новизна одержаних результатів

Дисертаційна робота містить результати, що характеризуються науковою новизною та спрямовані на підвищення ефективності інтелектуального аналізу мережевого трафіку в критичних середовищах. До основних здобутків слід віднести:

- *Вперше* запропоновані моделі прогнозування і виявлення кібербезпекових аномалій та визначення їх критичності, які за рахунок автоенкодерів та процедури формування динамічних порогів аномальності мережі, дозволяють формалізувати процес виявлення відхилень та відповідно оцінити влив на стан кібербезпеки системи;

- *Вперше* запропоновано математичну модель семантичної атрибуції кіберінцидентів у системах виявлення аномалій, яка за рахунок процедур вирахування коефіцієнтів аномальності, інтерпретації у контексті типів порушень, порівняння зі структурою активів критичної інфраструктури, дозволяє визначити множину вхідних і вихідних параметрів для формалізації процесу критичності кіберінцидентів;

- *Вперше* запропоновані методи виявлення аномалій та оцінювання їх критичності в режимі реального часу, які за рахунок етапів попередньої обробки даних, навчання автоенкодера, реконструкції даних, обчислення рівня аномальності, прогнозу значень мережевого трафіку, розрахунку стандартного відхилення похибок прогнозу, встановлення адаптивних меж аномальності, виявлення аномалій та відповідно підрахунку аномальних значень, обчислення рівня критичності, визначення категорій критичності та прийняття рішень , дозволило ранжувати події за рівнем небезпеки, скоротити час реагування в процесі інциденту, зменшити кількість хибнопозитивних спрацьовувань, стабілізувати часову стійкість детекції, підвищити рівень коректного розпізнавання загроз різної інтенсивності та відповідно визначити рівень загрози кіберінциденту;
- *Вперше* запропоновано узагальнену модель інтелектуальної системи прогнозування та виявлення аномалій, яка за рахунок модулів збору телеметрії, автоенкодера, Multilayer Perceptron, агрегатора аномалій, семантичної атрибуції та оцінювання критичності, дозволяє здійснювати пріоритизацію реагування та підвищити ефективність управління кібербезпекою об'єктів критичної інформаційної інфраструктури.

3 Практичне значення отриманих результатів

Створено програмо-алгоритмічний комплекс потокової аналітики для виявлення та короткострокового прогнозування аномалій мережевого трафіку різної інтенсивності з адаптивним порогуванням, виявленням concept drift, семантичною атрибуцією (у т.ч. MITRE ATT&CK) і ризик-скорингом; передбачено API для інтеграції з SIEM/SOAR, роботу у metadata-driven режимі над шифрованими протоколами (TLS 1.3/HTTP-2/QUIC) та розгортання on-prem/edge/cloud.

Апробацію результатів виконано в межах тематичних НДР ДУІКТ та у навчальному процесі кафедри технічних систем кіберзахисту: підготовлено лабораторні роботи/кейси з аналізу трафіку IT/OT, сформовано навчальний стенд з елементами ICS/SCADA для відтворення типових сценаріїв інцидентів.

Експериментальна валідація на відкритих наборах і стендових даних показала зменшення частки хибних сповіщень, скорочення MTTA/MTTR і підвищення стабільності алерт-стріму за рахунок гібридної моделі та адаптивної калібровки; сформовано референтні сценарії тестування для подальших впроваджень.

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), й "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

Дисертація присвячена вирішенню актуальної задачі розробці інтегрованої інтелектуальної системи виявлення аномалій у мережевому трафіку, яка поєднує моделі прогнозування, семантичної атрибуції та динамічного визначення критичності з практичними методами потокового аналізу та процедурою обробки кіберінцидентів.

Розв'язання даної задачі дозволяє підвищити ефективність захисту інформаційних систем і критичної інфраструктури в умовах зростання

складності атак та обсягів мережевого трафіку шляхом інтеграції сучасних методів глибокого навчання з адаптивним механізмом аналізу критичності подій.

Достовірність наукових положень, висновків і рекомендацій підтверджується узгодженістю теоретичних досліджень з результатами імітаційного моделювання, практичною імплементацією розроблених моделей і методів, результатами експериментів, які узгоджуються з даними відомих досліджень.

5 Повнота оприлюднення результатів дисертаційної роботи

Основні результати дисертаційної роботи Рижакова М.М. достатньо повно викладені у 12 друкованих працях у наукових журналах, включених до «Переліку фахових видань України». Опубліковані матеріали охоплюють ключові компоненти дослідження: інтелектуальні методи виявлення аномалій, узагальнену модель системи та підхід до оцінювання критичності подій.

6 Загальна характеристика структури та змісту дисертаційної роботи

Дисертація складається із вступу, чотирьох розділів та висновків до них, а також бібліографії, що містить 131 посилань на 9 сторінках. Загальний обсяг роботи становить 179 сторінки, з них 136 сторінки основного тексту, 9 рисунків, 18 таблиць.

У вступі зазначено актуальність теми дисертації, сформульовано мету і задачі досліджень, заявлено наукову новизну та практичне значення отриманих результатів, перелік публікацій та апробації результатів роботи.

Перший розділ дисертації зосереджений на всебічному аналізі поточного стану сучасних методів, моделей і систем виявлення аномалій, що застосовуються у світовій практиці. Розглянуто сигнатурні, статистичні, поведінкові та глибинні підходи до детектування загроз, проведено порівняння промислових рішень класів IDS/IPS, NDR, SIEM, SOAR, XDR та

хмарних систем аналітики. Визначено їх обмеження, переваги й актуальні виклики, що зумовило формування вимог до інтелектуальної системи нового покоління.

У другому розділі проводиться вивчення комплексу моделей, що становлять теоретичну основу системи. Запропоновано моделі прогнозування мережевого трафіку на основі глибинних нейронних мереж, та динамічного визначення критичності, яка встановлює рівень ризику інциденту з урахуванням контексту, інтенсивності, впливу та можливості ескалації. Сформовано модель семантичної атрибуції кіберінцидентів, що забезпечує визначення аномалій через зіставлення їх із базами знань про загрози та поведінковими патернами.

У третьому розділі дисертації запропоновано практичні методи та алгоритми, що реалізують механізми виявлення аномалій на рівні потоків і груп пакетів. Описано процедури фільтрації, методи обробки часових рядів, алгоритми оцінки поведінкових характеристик, а також механізми раннього виявлення загроз. Розроблено покращені методи аналізу взаємозв'язків між подіями, визначення причинно-наслідкових зв'язків та формування структурованих ознак для подальшого класифікування.

Четвертий розділ присвячений розв'язанню питань, які пов'язані з конструюванням інтелектуальної системи виявлення аномалій. Проведено експериментальну оцінку ефективності системи на реальних та симульованих даних. Наведений приклад практичної апробації, яка підтвердила можливість інтеграції системи в SOC/SIEM середовища та її ефективність для задач моніторингу та реагування.

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 Рижакова М.М. є завершеним і повним дослідженням, яке містить теоретичні розробки та відповідні їм експериментальні перевірки.

7 Зауваження по дисертаційній роботі

1. З дисертаційної роботи (п.1.2) не зрозуміло, яким чином проводиться виділення та окремий аналіз “повільних” і малопомітних сценаріїв атак (low-and-slow), які є типовими для проникнення в сегменти об’єктів КІІ (тривалі розвідки, слабошумні ексфільтрації, повільні горизонтальні переміщення). Було б корисно навести окремий перелік таких сценаріїв, описати їхні характерні мережеві прояви та показати, які саме ознаки/агрегації роблять модель чутливою до них.

2. В п.2.1 запропонована модель виявлення аномалій, яка базується на використанні архітектур різних типів – багатошарових персептронів (MLP), рекурентних нейронних мереж (RNN, LSTM, GRU), автоенкодерів – забезпечує універсальність і гнучкість під час обробки даних. Але не зрозуміло яким чином виконується вибір необхідної мережі, та яким чином визначаються її вхідні параметри. Також не зрозуміло у чому полягає критерій універсальності запропонованої моделі.

3. В п. 2.2 дисертації запропонована модель семантичної атрибуції кіберінцидентів у системах виявлення аномалій на основі глибокого навчання, яка забезпечує підвищення ефективності ідентифікації кіберінцидентів шляхом розроблення та інтеграції вперше запропонованої автоматизованої математичної моделі семантичної атрибуції у глибинну систему виявлення аномалій. Але зі змісту не зрозуміло за якими критеріями визначається підвищення ефективності ідентифікації кіберінцидентів та які кількісні показники підтверджують підвищення ефективності.

4. В дисертаційної роботі запропоновано визначення рівня критичності за часткою аномалій, стр. 82 (вираз 2.70), але не зрозуміло яким чином визначені рівня, та які саме аномалії відносяться до кожного з рівнів критичності. Також не зрозуміло як ці результати впливають на безперервність бізнес-процесів об'єкту критичної інфраструктури.

5. У п. 3.1 дисертації запропонований метод адаптивного визначення меж аномальності ґрунтується на інтеграції глибинних нейронних мереж і автоенкодера із використанням статистичного аналізу похибок реконструкції. Але не зрозуміло які сема нейронні мережі використовуються та які вхідні данні потрібні, з урахування запропонованої класифікації рівнів критичності аномалій.

6. З дисертаційної роботи не зрозуміло чому у подальших моделях та методах (наприклад, метод семантичної атрибуції кіберінцидентів, стор. 100–111) не використовуються запропоновані рівні критичності аномалій (замість запропонованих чотирьох використовуються два або три рівня критичності).

7. На рис. 4.1 наведена узагальнена структура моделі системи прогнозування та виявлення аномалій у кіберінфраструктурі на основі глибокого навчання, але не зрозуміло яким чином моделі забезпечують побудову системи, а також яким чином рівні критичності є механізмом регулювання.

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 Рижакова Миколи Миколайовича відповідає

чинним вимогам, які встановлені у «Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах)», затвердженого постановою Кабінету Міністрів України від 19 травня 2023 року № 502, та "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).

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

- дисертаційна робота Рижакова Миколи Миколайовича є завершеною науковою працею, в якій отримані нові науково обґрунтовані результати, які дозволяють підвищити рівень захищеності даних на об'єктах критичних інформаційних інфраструктур;

- автор дисертаційної роботи Рижаков Микола Миколайович заслуговує на присудження наукового ступеня доктора філософії 125 – «Кібербезпека та захист інформації».

Офіційний опонент:
Доктор технічних наук, професор,
Лауреат національної премії ім. Бориса Патона
завідувач кафедри кібербезпеки,
Національний технічний університет
«Харківський політехнічний інститут» Сергій ЄВСЕЄВ

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

ЗАСВІДЧУЮ:
ВЧЕНИЙ СЕКРЕТАР
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"
Підпис
"___" _____ 20____ р.