ЗАТВЕРДЖУЮ
Перший проректор Державного університету інформаційно-комунікаційних технологій
член-кореспондент НАН України,
доктор технічних наук, професор,
лауреат Державної премії України в галузі науки і техніки,
Заслужений діяч науки і техніки України
_____ Олександр КОРЧЕНКО
"13" листопада 2025 року

ВИСНОВОК

міжкафедрального семінару кафедри Технічних систем кіберзахисту Державного університету інформаційно-комунікаційних технологій про наукову новизну, теоретичне та практичне значення результатів дисертаційної роботи
Рижакова Миколи Миколайовича на тему: "Методи та моделі виявлення аномалій мережевого трафіку на об'єктах критичних інформаційних інфраструктур", поданої на здобуття наукового ступеня доктора філософії в галузі знань
12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації

Витяг
з протоколу № 6 засідання кафедри Технічних систем кіберзахисту
від "30" жовтня 2025 року

Присутні: Головуючий на засіданні – директор Навчально-наукового інституту кібербезпеки та захисту інформації, д.т.н., професор Іванченко Євгенія Вікторівна.
З кафедри Технічних систем кіберзахисту:
завідувач кафедри – д.т.н., професор Туровський Олександр Леонідович;
професор кафедри – к.т.н., доцент Пепа Юрій Володимирович;
професор кафедри – к.т.н., доцент Іванченко Ігор Сергійович;
доцент кафедри – к.е.н. Аверічев Ігор Миколайович;
старший викладач кафедри – доктор філософії за спеціальністю 125 Кібербезпека та захист інформації Поночовний Петро Михайлович;
Запрошені:
- *з кафедри Управління кібербезпекою та захистом інформації:*
завідувач кафедри – д.е.н., професор Легомінова Світлана Володимирівна;
професор кафедри – д.т.н., професор Савченко Віталій Анатолійович;
доцент кафедри – к.т.н., доцент Щавінський Юрій Віталійович;
старший викладач – Примаченко Діана Володимирівна;

доцент кафедри – доктор філософії за спеціальністю 125 Кібербезпека та захист інформації Запорожченко Михайло Михайлович;

- *з кафедри Систем та технологій кібербезпеки:*

завідувач кафедри – д.т.н., професор Гайдур Галина Іванівна;
професор кафедри – д.т.н., професор Зибін Сергій Вікторович;
доцент кафедри – доктор філософії за спеціальністю 125 Кібербезпека та захист інформації Марченко Віталій Вікторович;
старший викладач – Бойко Анна Олександрівна.

Всього присутніх – 16 осіб, серед присутніх 4 докторів технічних наук, 1 доктор економічних наук, 3 кандидати технічних наук, 1 кандидат економічних наук та 3 доктора філософії.

ПОРЯДОК ДЕННИЙ:

Обговорення дисертаційної роботи аспіранта кафедри Технічних систем кіберзахисту Державного університету інформаційно-комунікаційних технологій Рижакова Миколи Миколайовича на тему: “Методи та моделі виявлення аномалій мережевого трафіку на об’єктах критичних інформаційних інфраструктур”, поданої на здобуття ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації.

Дисертація виконана на кафедрі Технічних систем кіберзахисту Державного університету інформаційно-комунікаційних технологій. Тема дисертаційної роботи затверджена в новій редакції та призначено наукових керівників:

кандидат технічних наук, доцент, професор кафедри Технічних систем кіберзахисту ІВАНЧЕНКО Ігор Сергійович;

доктор історичних наук, професор, ректор Державного університету інформаційно комунікаційних технологій ШУЛЬГА Володимир Петрович.

СЛУХАЛИ: доповідь про дисертаційну роботу Рижакова Миколи Миколайовича “Методи та моделі виявлення аномалій мережевого трафіку на об’єктах критичних інформаційних інфраструктур”, подану на здобуття ступеня доктора філософії за спеціальністю 125 Кібербезпека та захист інформації.

РИЖАКОВ М.М.: Шановні Голово, члени міжкафедрального семінару, присутні! Вашій увазі пропонується доповідь за дисертаційною роботою на тему: “Методи та моделі виявлення аномалій мережевого трафіку на об’єктах критичних інформаційних інфраструктур”.

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). Спільною рисою є зсув поведінкових патернів трафіку, що негативно впливає на доступність, цілісність і безперервність технологічних процесів та створює істотні економічні ризики для операторів критичних інформаційних інфраструктур. Попри прогрес у моніторингу та реагуванні, значна частина рішень залишається орієнтованою на сигнатури або на явні прояви високої інтенсивності. В умовах шифрування (TLS 1.3, HTTP/2, QUIC, DoH/DoT), гібридних IT/OT-середовищ і обмежених ресурсів edge-пристроїв інформативність пакетних полів зменшується, а поведінка користувачів і сервісів стає нестабільною. Додаткові виклики зумовлюють дефіцит розмічених даних, наявність зсувів концепції (seasonality, зміни топологій/навантажень) та потреба у пояснюваності рішень для скорочення часу виявлення й обробки інцидентів у SOC.

Аналіз сучасних праць засвідчує, що проблема раннього виявлення та короткострокового прогнозування різнотипних аномалій і їхньої семантичної атрибуції для критичних інформаційних інфраструктур вирішена неповною мірою. Типові системи або не відрізняють тонкі поведінкові відхилення від нормального трафіку, або генерують надмірну кількість хибних сповіщень, що затримує реагування й призводить до помилкових блокувань. Актуальним є розроблення гібридних методів, які поєднують реконструкційні моделі та моделі короткострокового прогнозування, підтримують адаптивне порогування з контрольованою часткою хибнопозитивних спрацювань, виявляють зсуви концепції та забезпечують семантичну атрибуцію інцидентів (у т.ч. в термінах MITRE ATT&CK) з подальшим ризик-скорингом та інтеграцією у процеси SIEM/SOAR.

Основні проблеми, що зумовлюють актуальність дослідження, такі:

– різна інтенсивність і варіативність проявів аномалій, через що традиційні порогові/сигнатурні підходи дають запізніле спрацювання або пропуски;

– широке використання шифрування та новітніх протоколів, що обмежує DPI й потребує metadata-driven/поведінкових методів;

– гетерогенність середовищ КІІ (IT/OT, ICS/SCADA, хмара/edge) і різна критичність активів за умов обмежених обчислювальних ресурсів;

– нестабільність статистики трафіку (concept drift), сезонність та динамічні зміни конфігурацій;

– дефіцит якісно розмічених даних, необхідність безнаглядних/напівнаглядних підходів і генерації синтетичних вибірок;

– вимоги до пояснюваності та узгодження з процесами SOC (зменшення MTTA/MTTR, пріоритизація алертів);

– потреба у масштабованості й робастності до навмисних впливів на дані/моделі (ухилення, отруєння).

Отже, створення спеціалізованої інтелектуальної системи виявлення аномалій мережевого трафіку для об’єктів КІІ, що поєднує гібридні моделі детектування й прогнозування, адаптивне порогування, механізми виявлення зсувів концепції та семантичну атрибуцію з ризик-скорингом і інтеграцією в

SIEM/SOAR, є науково й практично значущим завданням. Очікувані результати сприятимуть підвищенню кіберстійкості критичних сервісів, зниженню хибних сповіщень і своєчасному попередженню потенційно небезпечних інцидентів.

Метою дослідження є підвищення ефективності виявлення аномалій мережевого трафіку шляхом інтеграції сучасних методів глибокого навчання з адаптивним механізмом аналізу критичності подій.

Для досягнення поставленої мети автором виконано наступні окремі завдання дослідження:

- аналіз сучасних методів та моделей виявлення аномалій мережевого трафіку;
- розробка моделей прогнозування і виявлення кібербезпекових аномалій та визначення їх критичності.
- розробка математичної моделі семантичної атрибуції кіберінцидентів у системах виявлення аномалій;
- розробка методів виявлення аномалій та оцінювання їх критичності в режимі реального часу;
- розробка узагальненої моделі інтелектуальної системи прогнозування та виявлення аномалій;
- розробка алгоритмічного та програмного забезпечення реалізації узагальненої системи прогнозування та виявлення кіберінцидентів і проведення експериментального дослідження з метою підтвердження достовірності теоретичних розробок і практичної ефективності запропонованих рішень;

Для досягнення поставленої мети у дисертаційній роботі особисто Миколой Рижаковим було одержано нові наукові результати:

вперше розроблено 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 розроблено 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 розроблено 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

Достовірність отриманих наукових результатів дає алгоритмічне забезпечення, яке реалізує узагальнену інтелектуальну систему прогнозування та виявлення кіберінцидентів, що дає можливість забезпечити потокову аналітику, формування ризикових оцінок і короткострокове прогнозування аномалій. Проведене експериментальне дослідження на відкритих наборах даних і симуляційних сценаріях критичних інформаційних інфраструктур підтвердило досягнення точності детекції 89,3 %, Recall = 0.947, Precision = 0.984, F1 = 0.893 та продемонструвала перевагу над існуючими рішеннями на 13,1 % за ключовими експлуатаційними метриками, включаючи точність, стійкість, швидкодію та здатність до роботи зі слабовираженими і довготривалими відхиленнями.

Доповідь закінчено. Дякую за увагу!

По завершенню доповіді Рижакову Миколі Миколайовичу присутніми були поставлені такі запитання:

1. Чому аномалії слабкої інтенсивності в мережевому трафіку критичних інфраструктур важко виявляти традиційними методами?
2. Які основні цілі та завдання ставилися під час розроблення моделей виявлення аномалій?
3. Чому сигнатурні та порогові системи виявляються неефективними у випадку нових або слабовиражених загроз?
4. У чому полягає наукова новизна запропонованих моделей і методів?
5. Які типи ознак і метаданих використовувалися під час побудови моделей аналізу трафіку?
6. Які нейронні мережі та архітектури застосовано у розроблених моделях (AE, LSTM, Transformer тощо)?
7. Які результати експериментальних досліджень підтвердили ефективність розробленої системи?
8. Які переваги має запропонована система порівняно з існуючими IDS/NDR-рішеннями (наприклад, Suricata, Zeek, Darktrace)?
9. Як у роботі оцінюється ймовірність виникнення та критичність кіберінцидентів?
10. У яких практичних сферах доцільно застосовувати результати дослідження?
11. Які технології та інструменти використовувалися для збору, попередньої обробки та анотації даних?

12. Які обмеження та припущення має запропонована інтелектуальна система?

13. Які метрики використовувались для оцінки якості моделей виявлення аномалій?

14. Які публікації, апробація або проєктні реалізації супроводжували дисертаційне дослідження?

15. Де вже впроваджено або може бути впроваджено результати роботи у реальних інфраструктурах?

На всі питання були дані вичерпні відповіді.

СЛУХАЛИ: відгук наукового керівника кандидата технічних наук, доцента Іванченка Ігора Сергійовича про дисертаційну роботу аспіранта Рижакова Миколи Миколайовича на тему: “Методи та моделі виявлення аномалій мережевого трафіку на об’єктах критичних інформаційних інфраструктур”, подану на здобуття ступеня доктора філософії за спеціальністю 125 Кібербезпека та захист інформації.

ІВАНЧЕНКО І.С.: Дисертаційна робота Рижакова Миколи Миколайовича “Методи та моделі виявлення аномалій мережевого трафіку на об’єктах критичних інформаційних інфраструктур” виконана у межах плану науково-дослідних робіт Державного університету інформаційно-комунікаційних технологій МОН України за темою “Шляхи підвищення ефективності захисту командно-телеметричної інформації безпілотних літальних апаратів” (№ держ. реєстрації 0123U100244, ДУІКТ, м. Київ).

У процесі підготовки дисертації Микола Рижаков проявив себе як самостійний, наполегливий, відповідальний і високоерудований науковець, здатний формулювати та ефективно вирішувати складні наукові завдання. Він володіє сучасними методами наукових досліджень, аналітичними підходами, а також комунікаційними та іншими професійними компетентностями, що дозволяють йому логічно і послідовно представляти результати власних досліджень, публікувати їх у вітчизняних та міжнародних наукових виданнях, брати участь у наукових дискусіях, демонструючи вміння аргументовано обґрунтовувати та відстоювати власні наукові досягнення.

Автором дослідження коректно визначено мету, завдання, об’єкт і предмет дисертаційної роботи, що забезпечило логічну та методологічно цілісну побудову всіх етапів дослідження. У процесі виконання роботи було ефективно застосовано комплексний підхід, який поєднує сучасні методи штучного інтелекту, теорію ймовірностей, аналіз часових рядів, методи реконструкції поведінкових ознак, семантичну атрибуцію кіберінцидентів та оцінювання їх критичності. Застосування гібридних нейронних мереж, автоенкодерів, адаптивного порогування та механізмів риск-скорингу забезпечило всебічне дослідження проблеми виявлення аномалій різної інтенсивності у мережевому трафіку критичних інформаційних інфраструктур. Під час роботи автором проведено тестування запропонованих моделей на потокових даних, отриманих

зі стендів, симуляційних сценаріїв та серверних середовищ, розгорнутих на різних платформах, що дозволило оцінити їх ефективність в умовах реальних навантажень. Такий підхід дав змогу не лише теоретично обґрунтувати новизну отриманих результатів, але й підтвердити їхню практичну придатність для оперативного застосування у сфері кіберзахисту. Забезпечено комплексне дослідження точності, повноти, стійкості до дрейфу трафіку, здатності виявляти слабовиражені довготривалі аномалії та можливості інтеграції моделей у системи класу SOC/SIEM/SOAR.

У ході виконання дисертації автором повністю досягнуто поставленої мети — підвищення ефективності виявлення й прогнозування аномалій мережевого трафіку та забезпечення семантичної інтерпретації кіберінцидентів у режимі реального часу. Розроблені методи та моделі дали змогу зменшити кількість хибнопозитивних сповіщень, підвищити точність і стабільність детекції, сформувати систему раннього попередження та обґрунтованого ранжування загроз за рівнем критичності. Отримані результати мають суттєве практичне значення для фахівців у галузях кібербезпеки, інформаційної безпеки, управління інцидентами, аудиту інформаційних систем та експлуатації критичних інфраструктур. Запропоновані рішення можуть бути інтегровані у платформи моніторингу мережевого трафіку, системи автоматизованого реагування та освітні курси для підготовки аналітиків SOC та інженерів із кіберзахисту. Застосування матеріалів дослідження у навчальному процесі сприятиме підвищенню рівня професійної підготовки спеціалістів і формуванню сучасної компетентності у протидії складним і низькоінтенсивним кіберзагрозам.

За результатами дисертаційних досліджень опубліковано 12 наукових праць. Основні наукові результати викладені в 5 наукових статтях опублікованих у спеціалізованих фахових виданнях, затверджених наказом МОН України. Матеріали виступів на наукових та науково-практичних конференціях опубліковано у 3 збірниках тез доповідей.

Основні наукові та прикладні результати дисертаційної роботи, що виносяться на захист, отримані автором особисто. З наукових праць, які опубліковані у співавторстві, використано лише ті положення, ідеї та висновки, які є результатом власного дослідження здобувача.

Робота є самостійно виконаним науковим дослідженням, що відповідає принципам академічної доброчесності та не містить некоректних запозичень. Вона повністю відповідає спеціальності 125 Кібербезпека та захист інформаціїї, за якою подається до захисту.

Дисертаційна робота Рижакова Миколи Миколайовича є завершеним науковим дослідженням, що робить вагомий внесок у розвиток теоретичних і прикладних аспектів кібербезпеки, зокрема у сфері виявлення, прогнозування та семантичної атрибуції аномалій мережевого трафіку на об’єктах критичних інформаційних інфраструктур. Запропоновані автором науково-методичні підходи сприяють удосконаленню сучасних систем моніторингу, підвищенню точності виявлення слабовиражених кіберзагроз, забезпеченню коректної оцінки критичності інцидентів та формуванню адаптивних механізмів

реагування. Розроблені моделі та методи – зокрема гібридні нейронні архітектури, алгоритми семантичної атрибуції, механізми адаптивного порогування та ризик-скорингу – демонструють високу ефективність у реальних умовах функціонування мережевих інфраструктур. Дисертаційне дослідження відзначається актуальністю, науковою новизною і практичною значущістю, відкриваючи нові можливості для підвищення стійкості критичних сервісів до різнотипних кіберзагроз.

Робота виконана на високому науковому рівні, засвідчує наукову зрілість, ґрунтовну підготовку та високу професійну компетентність здобувача у галузі кібербезпеки. Отримані результати можуть бути використані в галузевих центрах моніторингу безпеки, у системах SOC/SIEM/SOAR, при експлуатації критичних інформаційних інфраструктур, а також у навчальному процесі підготовки фахівців з інформаційної та кібербезпеки.

Вважаю, що дисертаційна робота повністю готова до захисту, а її автор заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 125 Кібербезпека та захист інформації.

Призначені рецензенти:

к.т.н., доцент, професор кафедри Технічних систем кіберзахисту Пепа Юрій Володимирович; д.т.н., професор, професор кафедри Систем та технологій кібербезпеки Зибін Сергій Вікторович загалом позитивно оцінили дисертаційну роботу, відзначивши її високу актуальність, теоретичну значущість та практичну цінність. Особливу увагу було приділено науковій новизні, обґрунтованості результатів і систематизованому підходу до вирішення поставленої проблеми.

Зокрема, **доктор технічних наук, професор, професор кафедри Систем та технологій кібербезпеки Зибін Сергій Вікторович** відзначив високий науковий рівень дисертаційної роботи Рижакова Миколи Миколайовича та її актуальність у контексті сучасних викликів кібербезпеки.

Загальний аналіз дисертації дозволив зробити наступні висновки:

1. Ознайомлення зі змістом дисертаційної роботи підтверджує логічність її побудови, чіткість наукової аргументації, а також обґрунтованість висновків і рекомендацій, сформульованих автором самостійно.

2. Структура роботи відповідає визначеній меті та поставленому науковому завданню. Дисертація ґрунтується на положеннях кібербезпеки, теорії аномалій, аналізу поведінкових моделей трафіку, теорії математичного моделювання, що забезпечує її теоретичну глибину. Актуальність дослідження підтверджується проведеним аналізом сучасних систем моніторингу, де за певними ознаками ми бачимо, що створення інтелектуальної системи виявлення та прогнозування аномалій є важливим і необхідним для підвищення стійкості критичних інформаційних інфраструктур.

3. Автором сформульовано оригінальні наукові рішення, спрямовані на створення інтелектуальної системи виявлення та прогнозування аномалій мережевого трафіку на об’єктах критичної інфраструктури. Це реалізовано у запропонованій моделі, що поєднує гібридні нейронні мережі та семантичну атрибуцію. Система аналізує поведінкові відхилення й визначає їх критичність.

Отримані результати мають значний потенціал для підвищення кіберстійкості інфраструктури

4. Дисертаційне дослідження є самостійною науковою працею, що не містить некоректних запозичень. Опубліковані результати досліджень відображають основні положення наукової новизни та відповідають вимогам до дисертацій за спеціальністю 125 Кібербезпека та захист інформації.

Позитивно оцінюючи положення дисертаційного дослідження Рижакова М.М., **Зибін С.В.** звернув увагу на певні аспекти, що можуть бути уточнені або розширені:

1. У роботі приділено значну увагу технічним аспектам виявлення, прогнозування та інтерпретації аномалій мережевого трафіку, однак аналіз специфіки саме слабовиражених та довготривалих поведінкових відхилень (low-intensity, stealth, long-duration anomalies), а також їх відмінностей від класичних різко виражених загроз потребує певного поглиблення. Було б корисно детальніше розглянути конкретні механізми формування таких аномалій (наприклад, повільне накопичення нестандартних метрик, аномалії сесійного рівня, приховані зміни патернів взаємодії), а також їхній вплив на здатність обходити традиційні порогові та сигнатурні системи захисту.

2. У роботі ґрунтовно досліджено принципи функціонування розробленої інтелектуальної системи, однак доцільно було б глибше проаналізувати вплив динамічно змінюваних умов мережевого середовища, таких як різкі піки легітимного трафіку, сезонна варіативність навантаження, зміна маршрутизації чи топології мережі, на точність виявлення слабовиражених аномалій та ймовірність хибної атрибуції або помилкової оцінки критичності кіберінцидентів.

3. Дослідження має суттєвий прикладний потенціал, проте було б доцільно ширше розглянути питання практичної інтеграції запропонованої системи в існуючу інфраструктуру кіберзахисту критичних інформаційних ресурсів (наприклад, у поєднанні з SIEM/SOC-платформами, NDR-рішеннями або системами інцидент-менеджменту), а також визначити конкретні вимоги до обчислювальних ресурсів, масштабованості та керованості системи в різних умовах її експлуатації.

Наведені зауваження стосуються насамперед аспектів подальшого розвитку наукової тематики й не зменшують загальної цінності виконаного дослідження. Робота є завершеним науковим дослідженням, що робить вагомий внесок у розвиток методів виявлення, прогнозування та семантичної інтерпретації складних для детектування аномалій мережевого трафіку й підвищення кіберстійкості критичних інформаційних інфраструктур. За рівнем наукової аргументації, методологічного опрацювання та практичної значущості отриманих результатів, дисертація відповідає вимогам, що висуваються до досліджень на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека та захист інформації». Робота виконана державною мовою з дотриманням норм академічної доброчесності.

Кандидат технічних наук, доцент, професор кафедри Технічних систем кіберзахисту Пепа Юрій Володимирович охарактеризував дисертаційну

роботу як ґрунтовне наукове дослідження високого рівня, що відображає актуальні виклики у сфері кібербезпеки, зокрема проблему виявлення та інтерпретації складних для детектування аномалій мережевого трафіку у критичних інформаційних інфраструктурах. Робота містить чітке теоретичне обґрунтування, сучасні підходи до аналізу поведінкових відхилень, механізми семантичної атрибуції кіберінцидентів та практичні рішення щодо оцінювання їх критичності. Наукові результати дослідження мають важливе значення для розвитку інтелектуальних систем моніторингу, підвищення кіберстійкості інфраструктур та впровадження в організаціях різного профілю.

Разом із позитивною оцінкою дисертації, рецензент висловив окремі зауваження та наголосив на перспективах подальших досліджень:

1. Універсальність системи. Запропонований механізм виявлення слабовиражених аномалій орієнтований на загальні закономірності поведінкового трафіку. Доцільно було б перевірити його ефективність у різних типах середовищ, таких як високонавантажені промислові мережі, розподілені SCADA-системи, платформи з інтенсивним API-обміном або середовища з динамічно змінними шаблонами легітимної активності, де профілі трафіку можуть відрізнятися від стандартних.

2. Часова динаміка аномалій. У роботі переважно аналізуються стаціонарні сценарії формування відхилень. Доцільним є поглиблене дослідження впливу часових факторів — тривалості аномалії, нерівномірності зміни поведінкових ознак, сезонних коливань навантаження, адаптивних моделей порушень — на стійкість системи до довготривалих і повільно накопичуваних аномалій, які можуть імітувати поведінку коректного трафіку.

3. Оптимізація роботи системи. Дослідження фокусується на алгоритмах детектування та атрибуції, однак потребує розширеного аналізу ефективності різних стратегій реагування, зокрема динамічного управління порогами, адаптивного ризик-скорингу, інтеграції з SIEM/SOC-рішеннями або механізмами автоматизованого блокування. Варто визначити оптимальні параметри калібрування для зменшення ймовірності хибнопозитивних сповіщень у реальних умовах експлуатації.

Загалом, рецензована робота виконана на високому науковому рівні, вирізняється системністю, новизною технічних рішень та практичною цінністю отриманих результатів, проведена з дотриманням норм академічної доброчесності. Це дає підстави оцінити її позитивно та рекомендувати до захисту на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека та захист інформації».

Рецензентами відзначено, що дисертаційна робота відповідає встановленим вимогам щодо наукової новизни, теоретичної та практичної значущості, а також може бути рекомендована до спеціалізованої вченої ради для попереднього розгляду та захисту на здобуття наукового ступеня доктора філософії.

ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертаційної роботи Рижакова Миколи Миколайовича на тему “ Методи та моделі виявлення аномалій мережевого трафіку на об’єктах критичних інформаційних інфраструктур ”, поданої на здобуття ступеня доктора філософії за спеціальністю 125 Кібербезпека та захист інформації

Актуальність теми дослідження. 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). Спільною рисою є зсув поведінкових патернів трафіку, що негативно впливає на доступність, цілісність і безперервність технологічних процесів та створює істотні економічні ризики для операторів критичних інформаційних інфраструктур. Попри прогрес у моніторингу та реагуванні, значна частина рішень залишається орієнтованою на сигнатури або на явні прояви високої інтенсивності. В умовах шифрування (TLS 1.3, HTTP/2, QUIC, DoH/DoT), гібридних IT/OT-середовищ і обмежених ресурсів edge-пристроїв інформативність пакетних полів зменшується, а поведінка користувачів і сервісів стає нестабільною. Додаткові виклики зумовлюють дефіцит розмічених даних, наявність зсувів концепції (seasonality, зміни топологій/навантажень) та потреба у пояснюваності рішень для скорочення часу виявлення й обробки інцидентів у SOC.

Аналіз сучасних праць засвідчує, що проблема раннього виявлення та короткострокового прогнозування різнотипних аномалій і їхньої семантичної атрибуції для критичних інформаційних інфраструктур вирішена неповною мірою. Типові системи або не відрізняють тонкі поведінкові відхилення від нормального трафіку, або генерують надмірну кількість хибних сповіщень, що затримує реагування й призводить до помилкових блокувань. Актуальним є розроблення гібридних методів, які поєднують реконструкційні моделі та моделі короткострокового прогнозування, підтримують адаптивне порогування з контрольованою часткою хибнопозитивних спрацювань, виявляють зсуви концепції та забезпечують семантичну атрибуцію інцидентів (у т.ч. в термінах MITRE ATT&CK) з подальшим ризик-скорингом та інтеграцією у процеси SIEM/SOAR.

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

Дисертаційна робота виконана відповідно до планів наукової і науково-технічної діяльності Державного університету інформаційно-комунікаційних технологій в рамках науково-дослідної роботи “Шляхи підвищення ефективності захисту командно-телеметричної інформації безпілотних літальних апаратів” (№ держ. реєстрації 0123U100244, ДУІКТ, м. Київ).

Мета і завдання дослідження.

Метою дослідження є підвищення ефективності виявлення аномалій мережевого трафіку шляхом інтеграції сучасних методів глибокого навчання з адаптивним механізмом аналізу критичності подій.

Для досягнення поставленої мети автором виконано наступні *окремі завдання дослідження*:

аналіз сучасних методів та моделей виявлення аномалій мережевого трафіку;

розробка моделей прогнозування і виявлення кібербезпекових аномалій та визначення їх критичності.

розробка математичної моделі семантичної атрибуції кіберінцидентів у системах виявлення аномалій;

розробка методів виявлення аномалій та оцінювання їх критичності в режимі реального часу;

розробка узагальненої моделі інтелектуальної системи прогнозування та виявлення аномалій;

розробка алгоритмічного та програмного забезпечення реалізації узагальненої системи прогнозування та виявлення кіберінцидентів і проведення експериментального дослідження з метою підтвердження достовірності теоретичних розробок і практичної ефектичвності запропонованих рішень;.

Об’єкт дослідження – процес виявлення аномалій мережевого трафіку на об’єктах критичних інформаційних інфраструктур.

Предмет дослідження – методи та моделі виявлення аномалій мережевого трафіку.

Методи дослідження.

ґрунтуються на потоковій обробці мережевого трафіку з агрегуванням пакетів у флоу/запити в часових вікнах та побудові метаданих і поведінкових ознак (статистичних, протокольних, часових, ентропійних, графових), придатних і для шифрованих протоколів. Запропоновано гібридний підхід: реконструкційні моделі (AE/β-VAE) для виявлення відхилень структури ознак поєднано з моделями короткострокового прогнозування (LSTM/TCN/Transformer) для фіксації аномальної динаміки. Застосовано адаптивне порогування з контролем частки хибних сповіщень та виявлення зсувів концепції (наприклад, CUSUM/Page-Hinkley/ADWIN). Для семантичної атрибуції інцидентів використано граф знань і мапування на тактики/техніки MITRE ATT&CK з формуванням інтегрального ризик-скорингу.

Достовірність наукових результатів, висновків і рекомендацій забезпечено коректним використанням математичного апарату, крос-валідацією, бутстреп-оцінюванням довірчих інтервалів, абляційними дослідженнями та аналізом чутливості параметрів. Оцінювання проводилося за метриками Precision/Recall/F1, ROC-AUC/PR-AUC, latency, throughput, а також за стійкістю до навмисних впливів (ухилення, отруєння даних). Вплив різнотипних мережевих атак (L3/L4/L7-DDoS, сканування, brute-force, C2-beaconing, латеральні переміщення, ексфільтрація, аномалії промислових протоколів) досліджено за допомогою симуляцій і експериментального моделювання на відкритих наборах та стендах ICS/SCADA у різних сценаріях навантаження.

Результати теоретичних розробок підтверджено узгодженими показниками якості та відтворюваністю експериментів, що дозволило обґрунтувати практичну застосовність запропонованих методів для підвищення рівня захищеності КІІ.

Наукова новизна дослідження:

Вперше розроблено 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 розроблено 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 розроблено 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..

Практичне значення.

Практичне значення одержаних результатів полягає в тому, що 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.

Особистий внесок здобувача. Дисертація є самостійною науковою працею, в якій висвітлені власні ідеї і розробки автора, що дозволили вирішити поставлені завдання. Робота містить теоретичні та методичні положення і висновки, сформульовані дисертантом особисто. Використані в дисертації ідеї,

положення чи гіпотези інших авторів мають відповідні посилання і використані лише для підкріплення ідей здобувача.

Роботи, опубліковані у співавторстві, містять результати, з яких у дисертаційній роботі використано лише ті, що отримані безпосередньо здобувачем. У співавторських публікаціях автором виконано: розроблення методів і моделей виявлення та короткострокового прогнозування аномалій мережевого трафіку на об’єктах критичної інформаційної; побудова моделей прогнозування і виявлення кібербезпекових аномалій та визначення їх критичності на основі глибинного навчання; розроблення математичної моделі семантичної атрибуції кіберінцидентів у системах виявлення аномалій; розроблення методів виявлення аномалій та оцінювання їх критичності в режимі реального часу; розроблення узагальненої моделі (архітектури) інтелектуальної системи прогнозування та виявлення аномалій із модулями збору телеметрії, виявлення, агрегації, семантичної атрибуції та оцінювання критичності; алгоритмічна реалізація потокової аналітики та формування ризикових оцінок для практичного використання в середовищах SOC/SIEM.

Апробація результатів дослідження.

Основні результати дисертаційної роботи були представлені та обговорені на міжнародних науково-технічних та науково-практичних конференціях: XII Міжнародна науково-практична конференція «Актуальні питання забезпечення кібербезпеки та захисту інформації» (м. Київ, 2025 року), Міжнародна науково-практична конференція цифрова трансформація: посилення кібербезпекових спроможностей у сучасному світі (м. Київ, м. Краків, 2025 року), IV Міжнародна науково-технічна конференція «Безпека інформаційних технологій» (м. Львів, 2025 року).

Публікації. За результатами дисертаційних досліджень опубліковано 12 наукова праця. Основні наукові результати викладені в 5 наукових статтях опублікованих у спеціалізованих фахових виданнях, затверджених наказом МОН України. Матеріали виступів на наукових та науково-практичних конференціях опубліковано у 3 збірниках тез доповідей.

Список опублікованих праць за темою дисертації

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Зінченко О. В., Звенігородський О. С., Березівський М. Ю., Рижаков М. М. Методика порівняння та оцінювання протоколів маршрутизації мереж автомобільного транспорту. Зв'язок. № 6, с. 58–60, 2020. DOI: 10.31673/2412-9070.2020.065355

2. Катков Ю. І., Зінченко О. В., Рижаков М. М., Тесленко О. С. Критичні аспекти впровадження Smart Retail. Зв'язок. № 6, с. 34–41, 2019. DOI: 10.31673/2412-9070.2019.063441

3. Катков Ю. І., Березовська Ю. В., Рижаков М. М., Гнидюк Д. С. Аналіз ризиків застосування технологій віртуалізації і контейнеризації в хмарних сервісах. Зв'язок. № 5, с. 19–26, 2019. DOI: 10.31673/2412-9070.2019.051926

4. Катков Ю. І., Березовська Ю. В., Пшеничний Ю. С., Рижаков М. М., Прокопов С. В. Аналіз загроз та вразливостей під час впровадження технології 4G/LTE. Телекомунікаційні та інформаційні технології. № 4, с. 25–38, 2019. DOI: 10.31673/2412-4338.2019.042538

5. Шикула О. М., Рижаков М. М., Білоусова С. В., Литвинець В. В. Розробка сайту автосервісу з можливістю виклику евакуатора за даними геопозиціювання. Наукові записки Державного університету інформаційно-комунікаційних технологій. № 1–2, с. 54–62, 2022. DOI:10.31673/25187678.2022.025462.

6. Звенігородський О. С., Кутовий С. О., Прокопов С. В., Рижаков М. М. Якість обслуговування Інтернет речей у протоколі MQTT: особливості і процедури. Наукові записки Державного університету інформаційно-комунікаційних технологій. № 4, с. 80–85, 2019. DOI:10.31673/2518-7678.2019.048085.

7. Рижаков М., Поночовний П. Модель трансформації на основі ШІ з елементами захисту від DDoS-атак. Прикладні проблеми комп'ютерних наук, безпеки та математики, 4, с. 14–32, 2025.

8. Іванченко Є., Аверічев І., Рижаков М. Узагальнена модель прогнозування та виявлення кібербезпекових аномалій на основі ШІ. Кібербезпека: освіта, наука, техніка, 4(28), 529–546, 2025. https://doi.org/10.28925/2663-4023.2025.28.823

9. Шульга В., Іванченко Є., Аверічев І., Рижаков М. Методи інтелектуального виявлення аномалій і критичних ситуацій у кіберсистемах на основі глибокого навчання. Information Technology: Computer Science, Software Engineering and Cyber Security, № 2, с. 204–215, 2025. DOI:10.32782/IT/2025-2-21.

10. Туровський О., Рижаков М. Методичний підхід до комплексної ідентифікації та аналізу кіберзагроз трафіку в мережах 5G/IMT-2020 на основі технологій ШІ. Вимірювальна та обчислювальна техніка в технологічних процесах, (1), 267–277, 2025. https://doi.org/10.31891/2219-9365-2025-81-33

11. Шульга В., Іванченко І., Рижаков М. Узагальнена модель інтелектуальної системи прогнозування та виявлення аномалій у кіберінфраструктурі на основі глибокого навчання. Measuring and Computing Device, (3), 217–225, 2025. https://doi.org/10.31891/2219-9365-2025-83-28

12. Шульга В.П., Іванченко І.С., Рижаков М.М.. Математична модель семантичної атрибуції кіберінцидентів у системах виявлення аномалій на основі глибокого навчання, Сучасний захист інформації, 2025, No 3(63), 186 – 198. https://doi.org/10.31673/2409-7292.2025.032076.

Структура та обсяг дисертації.

Дисертаційна робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел із 131 найменувань на 9 сторінках. Загальний обсяг роботи становить 179 сторінок, серед яких 136 сторінок основного тексту, 9 рисунки, 18 таблиць.

Характеристика особистості здобувача.

Рижаков Микола Миколайович у 2019 році закінчив Державний університет телекомунікацій та отримав диплом Магістра за спеціальністю «Телекомунікації та радіотехніка» та здобув кваліфікацію інженер інформаційно-телекомунікаційних систем; викладач вищих навчальних закладів. У 2024 році вступив на здобувача поза аспірантурою Державного університету інформаційно-комунікаційних технологій, м. Київ, Україна, за спеціальністю 125 Кібербезпека та захист інформації. 16 вересня 2025 року на засіданні Вченої Ради Державного університету інформаційно-комунікаційних технологій було затверджено у новій редакції тему дисертаційної роботи Рижакова Миколи Миколайовича “Методи та моделі виявлення аномалій мережевого трафіку на об’єктах критичних інформаційних інфраструктур”.

Під час виконання дисертаційної роботи Рижаков М.М. провів ґрунтовне дослідження, спрямоване на аналіз сучасного стану проблематики, заявленої у дисертації. Було чітко визначено об’єкт, предмет, мету та завдання дослідження, обґрунтував актуальність теми та обрано відповідні методи для досягнення поставлених цілей. Здобувач Микола Рижаков приймав безпосередню участь під час постановки наукових завдань, планування та виконання експериментів, а також обговорення отриманих результатів. Проявив себе як відповідальний, дисциплінований та ініціативний дослідник, здатний працювати як самостійно, так і в команді. Продемонстрував високий рівень теоретичної підготовки, володіє сучасними методами дослідження, аналітичними інструментами та практичними навичками. Системно підходить до вирішення наукових завдань, критично оцінює результати власної роботи, виявляє наполегливість у досягненні поставлених цілей. Постійно вдосконалює свої знання, прагнучі підвищити рівень наукової обґрунтованості та практичної значущості отриманих результатів.

Оцінка мови та стилю дисертації. Дисертація виконана фаховою українською мовою, текстове подання матеріалу відповідає стилю науково-дослідної літератури.

Рецензенти рекомендують: відповідно до **п.15** Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого постановою Кабінету Міністрів України від 12 січня 2022р. №44, ***пропонується такий склад разової ради:***

Голова ради:

Савченко Віталій Анатолійович, доктор технічних наук, професор, професор кафедри Управління кібербезпекою та захистом інформації Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій.

Рецензенти:

Пепа Юрій Володимирович, кандидат технічних наук, доцент, професор кафедри Технічних систем кіберзахисту Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій.

Зибін Сергій Вікторович, доктор технічних наук, професор, професор кафедри Систем та технологій кібербезпеки Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій.

Офіційні опоненти:

Хлапонін Юрій Іванович, доктор технічних наук, професор, професор кафедри Інженерії програмного забезпечення та кібербезпеки Державного торговельно-економічного університету.

Євсеєв Сергій Петрович, доктор технічних наук, професор, завідувач кафедри Кібербезпеки Національного технічного університету «Харківський політехнічний інститут».

У результаті попередньої експертизи дисертації **Рижакова Миколи Миколайовича** і повноти публікації основних результатів дослідження.

УХВАЛЕНО:

1. Затвердити висновок про наукову новизну, теоретичне та практичне значення результатів дисертації Рижакова Миколи Миколайовича на тему “Методи та моделі виявлення аномалій мережевого трафіку на об’єктах критичних інформаційних інфраструктур”.

2. Констатувати, що за актуальністю, степенем наукової новизни, обґрунтованістю, науковою та практичною цінністю здобутих результатів дисертація Рижакова М.М. відповідає спеціальності 125 Кібербезпека та захист інформації та вимогам **Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах),** затвердженого постановою Кабінету Міністрів України від 23 березня 2016 р. № 261, пп. **6, 7, 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 Кабінету Міністрів України від 12 січня 2022 р. № 44.

3. Рекомендувати дисертацію Рижакова М.М. на тему “Методи та моделі виявлення аномалій мережевого трафіку на об’єктах критичних інформаційних інфраструктур” до захисту на здобуття ступеня доктора філософії у разовій спеціалізованій вченій раді за спеціальністю 125 Кібербезпека та захист інформації.

4. Рекомендувати вченій раді Державного університету інформаційно-комунікаційних технологій затвердити склад разової спеціалізованої вченої ради:

Голова ради:

Савченко Віталій Анатолійович, доктор технічних наук, професор, професор кафедри Управління кібербезпекою та захистом інформації Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій.

Рецензенти:

Пепа Юрій Володимирович, кандидат технічних наук, доцент, професор кафедри Технічних систем кіберзахисту Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій.

Зибін Сергій Вікторович, доктор технічних наук, професор, професор кафедри Систем та технологій кібербезпеки Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій.

Офіційні опоненти:

Хлапонін Юрій Іванович, доктор технічних наук, професор, професор кафедри інженерії програмного забезпечення та кібербезпеки Державного торговельно-економічного університету.

Євсеєв Сергій Петрович, доктор технічних наук, професор, завідувач кафедри Кібербезпеки Національний технічний університет «Харківський політехнічний інститут».

Результати голосування щодо рекомендації до захисту дисертації Рижакова Миколи Миколайовича:

"За" – 16

"Проти" – немає

"Утримались" – немає

Додаток: Презентація Рижакова Миколи Миколайовича на 28 стор.

Головуючий на засіданні –
Директор Навчально-наукового інституту
кібербезпеки та захисту інформації Євгенія ІВАНЧЕНКО

Секретар засідання Петро ПОНОЧОВНИЙ