РЕЦЕНЗІЯ

рецензента
доктора технічних наук, професора,
професора кафедри систем та технологій кібербезпеки
Навчально-наукового інституту кібербезпеки та захисту інформації
Державного університету інформаційно-комунікаційних технологій
ЗИБІНА Сергія Вікторовича
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"

Актуальність теми

Забезпечення кіберстійкості об'єктів критичної інформаційної інфраструктури (КІІ) в сучасних умовах належить до пріоритетних завдань національної безпеки та захисту критичних сервісів. Реальне мережне середовище характеризується високою динамікою, нерівномірністю навантаження, наявністю шумів, а також широким спектром атак, підходи реалізації яких постійно еволюціонують та ускладнюються. У таких умовах класичні підходи до виявлення аномалій, зокрема сигнатурні або суто статистичні, часто мають обмеження щодо адаптації до нових сценаріїв, контекстності оцінювання та пояснюваності результатів. У дисертаційному досліджені запропоновано підхід, орієнтований на створення інтелектуальної системи прогнозування, виявлення та семантичної атрибуції аномалій у мережному трафіку з використанням методів глибокого навчання, що безпосередньо спрямовано на підвищення надійності та захищеності КІІ. Важливо відмітити той аспект, що автором наголошено на поєднанні детектування та прогнозування при застосуванні адаптивного порогування, урахуванні зсувів концепції, а також семантичній атрибуції з ризик-скорингом та

можливістю інтеграції в SIEM/SOAR, що є практично значущим для сучасних SOC-процесів.

Отже, обрана тема дисертаційної роботи є актуальною, своєчасною та має суттєве значення для розвитку теорії і практики кібербезпеки, зокрема для задач моніторингу й реагування в критичних інформаційних інфраструктурах.

Обґрунтованість наукових результатів, висновків та рекомендацій

Рівень обґрунтованості положень, висновків і рекомендацій у дисертації визначається логічною побудовою дослідження, послідовним переходом від аналізу сучасних підходів та промислових рішень до формування вимог і розроблення власних моделей та методів. У роботі на системному рівні поєднано прогнозування трафіку, виявлення аномальних відхилень, семантичну інтерпретацію (атрибуцію) інцидентів та динамічне оцінювання критичності, що сприяє підвищенню якості управління інцидентами та пріоритезації реагування. Зміст дисертації відповідає заявленому об'єкту дослідження – процесу виявлення аномалій мережевого трафіку на об'єктах КІІ – та предметній спрямованості, оскільки результати зосереджені на методах, моделях і процедурних етапах детектування/прогнозування/оцінювання критичності в межах кіберінцидент-менеджменту

Новизна наукових результатів дослідження

Дисертаційне дослідження містить низку результатів, що характеризуються науковою новизною та мають прикладну цінність для практики кіберзахисту. Зокрема, у роботі отримано наступні ключові результати:

Вперше розроблено:

1. Математичну модель семантичної атрибуції кіберінцидентів у системах виявлення аномалій, яка на основі розрахунку коефіцієнтів аномальності, їх інтерпретації в контексті типів порушень та зіставлення зі структурою активів КІІ дає змогу формалізувати набір вхідних і вихідних параметрів для оцінювання критичності інцидентів.

2. Методи виявлення аномалій та оцінювання їх критичності в реальному часі, що охоплюють попередню обробку даних, навчання автоенкодера,

реконструкцію, визначення рівня аномальності, прогнозування значень трафіку, розрахунок похибок прогнозу та їх дисперсійних характеристик, формування адаптивних меж аномальності, підрахунок аномальних значень, визначення рівня критичності й категорій та прийняття рішення, що в сукупності дає можливість ранжувати події за рівнем небезпеки та знижувати кількість хибнопозитивних спрацювань.

3. Узагальнену модель інтелектуальної системи прогнозування і виявлення аномалій, яка інтегрує модулі збору телеметрії, автоенкодер, багатошаровий персептрон, агрегатор аномалій, семантичну атрибуцію та оцінювання критичності – з метою підвищення ефективності управління кібербезпекою об'єктів КІІ. Набуло подальшого розвитку (у межах системного бачення) ідея інтегрованої інтелектуальної системи виявлення аномалій у мережевому трафіку, яка поєднує прогнозні моделі, механізми атрибуції та динамічне оцінювання критичності із практичними методами потокового аналізу й обробки кіберінцидентів.

Таким чином, дисертаційне дослідження містить результати, які відповідають критеріям наукової новизни та можуть бути використані як основа для розвитку ризик-орієнтованих систем моніторингу й реагування в кіберінфраструктурах.

Практична цінність отриманих результатів

Практичне значення результатів полягає у можливості їх застосування для підвищення ефективності моніторингу кіберподій, зменшення хибнопозитивних спрацювань, підвищення точності ідентифікації аномалій та оптимізації пріоритезації інцидентів завдяки поєднанню семантичного аналізу й динамічного визначення критичності. У дисертації зазначено, що експериментальне оцінювання проводилось на реальних та симульованих даних, а практична апробація підтверджує можливість інтеграції системи в SOC/SIEM середовища для задач моніторингу та реагування. Крім того, автор підкреслює прикладну спрямованість підходу для високонавантажених інфраструктур, де критичною є здатність системи поєднувати точність прогнозних моделей, гнучкість методів глибинного аналізу та практичну цінність динамічної оцінки ризиків.

Зв'язок роботи з науковими програмами, планами та темами

Спрямованість дисертаційного дослідження узгоджується з вимогами чинного законодавства України у сфері кібербезпеки та захисту інформації, а також з державними стратегіями і програмами з підвищення кіберстійкості об'єктів критичної інфраструктури. Окремо відзначено кореляцію тематики роботи з міжнародними стандартами та підходами (ISO/IEC 27001/27035, IEC 62443, NIST тощо), що забезпечує можливість практичної інтеграції результатів у SOC/SIEM/SOAR. Дисертаційна робота виконується за планами наукової та науково-технічної діяльності ДУІКТ і в межах тематичних НДР кафедри (університету), пов'язаних із моделюванням кіберзагроз і створенням інтелектуальних систем моніторингу. Також у тексті дисертації вказано виконання відповідно до напряму НДР із конкретним номером держреєстрації.

Повнота викладу основних результатів дисертації у публікаціях

Основні результати дисертаційного дослідження відображені у наукових публікаціях здобувача, зокрема у працях, присвячених узагальненій моделі прогнозування та виявлення аномалій на основі ШІ, методам інтелектуального виявлення аномалій і критичних ситуацій на основі глибокого навчання, а також узагальненій моделі інтелектуальної системи для прогнозування і детектування аномалій у кіберінфраструктурі. Це свідчить про належний рівень апробації та наукової комунікації результатів.

Оцінка змісту дисертації та відповідність встановленим вимогам щодо оформлення

Дисертація є завершеною кваліфікаційною науковою працею, у якій сформульовано мету та реалізовано комплекс завдань, спрямованих на створення інтелектуальної системи прогнозування, виявлення і семантичної атрибуції аномалій у мережевому трафіку для підвищення надійності та захищеності об'єктів критичної інформаційної інфраструктури. В роботі окреслено технічні та методичні передумови актуальності задачі, наведено обґрунтування необхідності створення спеціалізованої системи для КІІ з поєднанням прогнозування і детектування, адаптивного порогування, семантичної атрибуції та ризик-скорингу з інтеграцією в

SIEM/SOAR. Така постановка проблеми є коректною, а підхід — сучасним і технологічно релевантним.

Недоліки та зауваження

Загалом позитивно оцінюючи наукове та практичне значення отриманих автором результатів, слід відзначити окремі дискусійні положення та висловити зауваження, що мають рекомендаційний характер і не знижують загальної позитивної оцінки дисертації:

1. У частині, де описується процедура адаптивного порогування та формування динамічних меж аномальності, доцільно було б більш детально регламентувати умови застосовності параметрів для різних типів трафіку (наприклад, за класами сервісів/сегментів КІІ) та надати розширені рекомендації щодо відтворюваного підбору гіперпараметрів у виробничих умовах.

2. Зважаючи на заявлену інтеграційну орієнтацію на SOC/SIEM/SOAR, корисним було б окремо систематизувати типові сценарії експлуатації (playbooks) – як саме результати семантичної атрибуції та критичності можуть автоматизувати прийняття рішень у режимі реального часу (на рівні правил, тригерів, реакцій).

3. Доцільним виглядало б розширення порівняльної частини експериментальної валідації за єдиною методологією (набір даних/метрики/затрати/латентність) із кількома сучасними NDR/UEBA-підходами, що дозволило б ще наочніше підкреслити переваги запропонованого рішення саме для КІІ.

4. Оскільки в роботі підкреслюється необхідність робастності до навмисних впливів на дані/моделі, варто було б ширше розкрити питання захисту ML-компонентів (ухилення/отруєння) у контексті практичного впровадження.

5. Певні терміни та визначення (зокрема пов'язані з інтерпретацією коефіцієнтів аномальності та їх віднесенням до типів порушень) бажано подати в максимально формалізованому вигляді (таблиці/правила відповідності), що покращило б прикладну відтворюваність методики.

Наведені зауваження мають уточнювальний характер і можуть бути враховані автором у подальших наукових дослідженнях та при розширенні прикладних впроваджень.

Висновок

Оцінюючи в цілому проведене автором дослідження, слід зазначити, що дисертаційна робота Рижакова Миколи Миколайовича на тему "Методи та моделі виявлення аномалій мережевого трафіку на об'єктах критичних інформаційних інфраструктур" є завершеним науковим дослідженням, у якому отримано нові науково обґрунтовані результати, що мають теоретичне та практичне значення для підвищення ефективності захисту об'єктів КІІ. За рівнем наукової новизни, обґрунтованістю висновків, практичною цінністю отриманих результатів, а також за змістом і спрямованістю дослідження дисертаційна робота відповідає вимогам до дисертацій на здобуття наукового ступеня доктора філософії, а її автор заслуговує присудження наукового ступеня доктора філософії за спеціальністю 125 – "Кібербезпека та захист інформації".

Рецензент:
професор кафедри систем та
технологій кібербезпеки
Державного університету інформаційно-
комунікаційних технологій
доктор технічних наук, професор Сергій ЗИБІН

Підпис док. техн. наук, професора С. Зибіна засвідчую.

Учений секретар
Державного університету інформаційно-
комунікаційних технологій Галина ЄНЧЕВА
«23» січня 2026 р.