КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1035
УДК 004.8:004.421:004.056:004.932

Чернящук Наталія Леонідівна
д.пед.н., професор
Волинський національний університет імені Лесі Українки, Луцьк, Україна
ORCID: 0000-0002-3178-8377
cherniashchuk.nataliia@vnu.edu.ua

МОДЕЛЬ АДАПТИВНИХ РЕКОМЕНДАЦІЙ ДЛЯ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ В IOT-СЕРЕДОВИЩАХ

Анотація. Системи рекомендацій для підтримки прийняття рішень у середовищах Інтернету речей (IoT) відіграють ключову роль у розвитку ефективних інтелектуальних рішень, забезпечуючи адаптивне управління кібербезпекою та оптимізацію ресурсів IoT-платформ. Особлива увага приділяється характеристикам даних IoT, які генеруються з численних джерел, таких як сенсори, комунікаційні пристрої та інші елементи інфраструктури, що формують великий обсяг гетерогенних даних. У роботі досліджуються сучасні методи рекомендацій, включно з колаборативною фільтрацією, підходами на основі контенту, глибокими нейронними мережами та ансамблевим навчанням, а також їх ефективність у реальних IoT-середовищах. Особлива увага приділяється проблемам масштабованості алгоритмів, продуктивності та оптимізації енергоспоживання в малопотужних пристроях. Мета дослідження полягає у розробці моделі адаптивних рекомендацій для підтримки прийняття рішень у IoT-середовищах із високим рівнем кіберзахисту. Для досягнення цієї мети проведено аналіз останніх наукових досліджень та рішень у галузі IoT і систем рекомендацій, вивчено сучасні платформи, що реалізують подібні підходи, визначено технології та методи, придатні для побудови системи рекомендацій, а також створено персоналізовану модель підтримки прийняття рішень. У роботі представлено інтеграцію методів машинного навчання, аналізу великих даних та інтелектуальної обробки інформації для забезпечення адаптивного реагування на кіберзагрози. Результати дослідження демонструють можливості поєднання показників компрометації, моделей інтелектуальних рекомендацій та алгоритмів прогнозування загроз для підвищення безпеки IoT-екосистем. Запропонована модель дозволяє не лише підвищити ефективність виявлення загроз та реагування на них у реальному часі, але й забезпечує інтелектуалізацію процесів управління, автоматизацію обслуговування та персоналізовану підтримку рішень для адміністраторів та користувачів IoT-систем. Дослідження підкреслює наукову та практичну значущість інтеграції адаптивних рекомендацій у сферу кібербезпеки IoT, забезпечуючи базу для подальшого розвитку гібридних рішень із використанням штучного інтелекту та методів обробки великих даних.

Ключові слова: IoT (Інтернет речей), система рекомендацій, персоналізовані рекомендації, IoT-екосистема, обробка даних, машинне навчання, аналітика великих даних, прийняття рішень, інтелектуальні системи, дані сенсорів.

ВСТУП

Інтернет речей (IoT) є однією з ключових сучасних технологій, що забезпечує взаємодію між мільярдами пристроїв, сенсорів і систем у різних сферах діяльності людини. Швидке зростання кількості IoT-пристроїв генерує величезні обсяги гетерогенних даних, які потребують ефективної обробки та аналізу для прийняття рішень у режимі реального часу. У цьому контексті особливо актуальним стає розроблення систем рекомендацій, здатних надавати інтелектуальну підтримку користувачам та адміністраторам систем.

Системи рекомендацій у IoT-середовищах виконують роль інструментів, що допомагають персоналізувати сервіси, оптимізувати використання ресурсів та підвищувати загальну ефективність роботи інфраструктури. На відміну від традиційних сфер застосування, таких як електронна комерція чи мультимедійні сервіси, IoT-середовища створюють додаткові виклики, включаючи високі темпи

генерації даних, обмежені ресурси пристроїв, необхідність масштабованості та низьке енергоспоживання.

Вирішення цих завдань потребує розроблення моделей систем рекомендацій, які інтегрують різноманітні підходи– від класичних методів фільтрації до сучасних алгоритмів машинного навчання та глибоких нейронних мереж. Таким чином, створення моделі системи рекомендацій для IoT-середовищ є важливим науковим і практичним завданням, що сприяє підвищенню інтелектуальності та автономності сучасних IoT-рішень.

Постановка проблеми. Сьогодні Інтернет речей (IoT) швидко розвивається, охоплюючи дедалі більше сфер людської діяльності – від «розумних» будинків і міської інфраструктури до промислових систем та охорони здоров'я. Широке підключення пристроїв, сенсорів та сервісів генерує великі обсяги даних, які потребують ефективного аналізу для прийняття рішень у режимі реального часу. У цьому контексті системи рекомендацій стають важливим інструментом інтелектуальної підтримки, оскільки вони допомагають виявляти корисні закономірності, надавати персоналізовані пропозиції та оптимізувати процеси.

Розробка моделі системи рекомендацій для IoT-середовищ є актуальною через низку викликів, таких як необхідність обробки великих обсягів гетерогенних даних, забезпечення масштабованості та продуктивності алгоритмів, а також врахування обмежених ресурсів вбудованих пристроїв. Важливим аспектом є також енергоспоживання, оскільки багато IoT-пристроїв працюють із обмеженими джерелами живлення.

Отже, створення моделі системи рекомендацій для IoT є своєчасним науковим і практичним завданням, оскільки воно поєднує обробку великих даних, інтелектуальний аналіз, оптимізацію ресурсів та підвищення ефективності прийняття рішень у складних розподілених середовищах.

Аналіз останніх досліджень та публікацій. Дослідження Rahmati [1] пропонує фреймворк кібербезпеки для IoT з використанням федеративного навчання, який забезпечує конфіденційність даних та виявлення загроз у реальному часі. Це демонструє тенденцію до розподілених інтелектуальних систем, де IoT-пристрої можуть адаптивно навчатися без централізованого збору чутливих даних.

Wu та співавт. [2] розробили адаптивну двонаправлену рекомендаційну мережу, яка автоматично оптимізує конфігурацію систем виявлення вторгнень в гетерогенних IoT-доменах, використовуючи адаптивну самонавчальну архітектуру. Це підкреслює актуальність самоадаптивних систем управління безпекою, що можуть підлаштовуватися під змінні умови мережі.

Lai та колеги [3] показали ефективність ансамблевого навчання для виявлення аномалій у IoT, що дозволяє враховувати чутливість гіперпараметрів для підвищення точності. Подібні методи корисні для адаптивних рекомендацій щодо захисту мережевого трафіку.

Mehedi та співавт. [4] запропонували глибоку трансферну модель для надійної системи виявлення вторгнень, що підкреслює необхідність інтеграції гнучких методів машинного навчання для адаптивного реагування на кіберзагрози.

Публікації Haidur та колег [5], Zhydka & Andriychenko [6], Merzlikin & Babeshko [7] та Dudykevych і співавт. [8] пропонують різні інтегральні моделі кібербезпеки для IoT-систем, включно з оцінкою ризиків, моніторингом трафіку та структурованим управлінням безпекою. Це створює основу для розробки адаптивних рекомендацій, що враховують реальний стан мережі та пристроїв.

G-lybovets та співавтори [9] аналізують вразливості та рішення для захисту, демонструючи, що для IoT-екосистем важливо інтегрувати інтелектуальні механізми виявлення загроз.

Zayats [10] та Pedan та колеги [11] досліджують використання штучного інтелекту та аналіз бездротових сигналів для покращення безпеки IoT, що підтверджує потребу в адаптивних моделях, які враховують динамічні характеристики мережі.

Shabala & Korniichuk [12] та Klyap і співавт. [13] досліджують оцінювання безпеки промислових IoT-об'єктів та міжнародні стандарти безпеки IoT-протоколів, що є критично важливим для адаптивних рекомендацій, оскільки моделі повинні враховувати регуляторні вимоги та потенційні ризики.

Pavlenko & Sribna [14] і Shabala [15] розробляють гібридні моделі IoT з підвищеним рівнем інформаційної безпеки, що демонструє тенденцію до поєднання аналітики даних, машинного навчання та протоколів безпеки для адаптивного управління кіберзахистом.

Мета статті – полягає у розробці моделі адаптивних рекомендацій для підтримки прийняття рішень у IoT-середовищах із високим рівнем кіберзахисту.

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

Більшість сучасних сценаріїв використання, особливо у сфері роздрібної торгівлі, можуть слугувати основою для формування практичних вимог, орієнтованих на магазини та точки продажу.

Оскільки структури збору та обробки даних у IoT-платформах принципово відрізняються від тих, що використовуються в маркетингових платформах, основним завданням є інтеграція цих даних у аналітичні системи. Тому інтеграційний модуль розглядається переважно у контексті взаємодії з IoT-пристроями, а не з маркетинговими платформами. Схема взаємодії систем обробки даних IoT разом з інтеграційним модулем показана на рисунку 1. Вона ілюструє реалізацію всіх попередньо описаних сценаріїв та відображає потоки даних між різними системами. Надалі детально обговорюється взаємодія модуля з кожним типом системи, а також вимоги та рекомендації до інформаційної системи.

Для класифікації вимог до системи використовується модель FURPS+, яка включає шість основних компонентів, а саме функціональні вимоги, вимоги до зручності використання, вимоги до надійності, вимоги до продуктивності, вимоги до підтримки.

Додатково символ «+» позначає додаткові обмеження, включаючи обмеження щодо проектування та реалізації, обмеження інтерфейсів, фізичні обмеження, а також правові та інші обмеження, що стосуються обробки персональних даних.

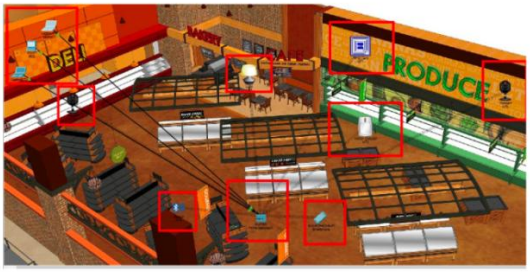

Рис. 1. Схема взаємодії системи обробки даних IoT для маркетингу на прикладі «розумного» магазину

Схема була розроблена та реалізована у Cisco Packet Tracer, мережевому симуляторі, створеному компанією Cisco Systems, який дозволяє створювати функціональні мережеві моделі, налаштовувати маршрутизатори та комутатори за допомогою команд Cisco IOS, а також забезпечує взаємодію кількох користувачів через хмару.

Представлена схема є емуляцією частини спроектованої системи та демонструє базові принципи взаємодії пристроїв. Управління IoT-пристроями здійснюється через смартфон, як показано на рисунках 2-3.

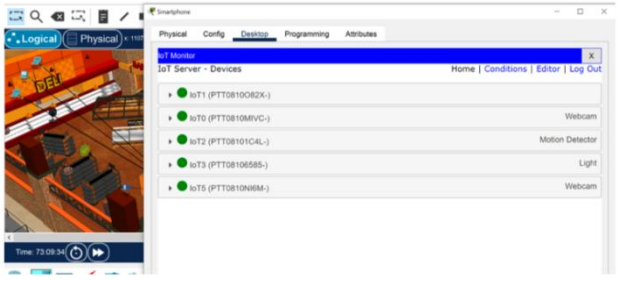

Рис. 2. Пристрої Інтернету речей (IoT) використані в системі

Рис. 3. Активація камери через смартфон та імітація розпізнавання клієнта

Основна функціональність застосунку полягає в забезпеченні інтеграції між різними платформами для реалізації сценаріїв та досягнення раніше описаних переваг. Схема взаємодії систем обробки даних IoT разом з інтеграційним модулем наведена на рисунку 1. Вона відображає частину реалізованих у

системі сценаріїв та демонструє потоки даних між різними компонентами. Розроблений та впроваджений модуль виявлення руху створено у середовищі Tinkercad. Модуль працює на основі PIR-датчика руху, підключеного до Arduino, а результати відображаються на LCD-дисплеї, як показано на рисунку 4.

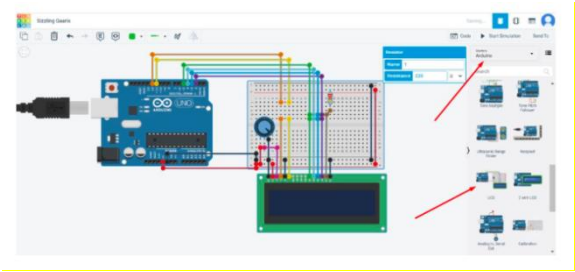

Рис. 4. Підключення LCD

Для забезпечення ефективного управління та обробки інформації у системі рекомендацій було розроблено веб-застосунок для адміністрування даних. Структура бази даних була спроектована відповідно до потреб веб-застосунку, із визначенням таблиць, полів та взаємозв'язків між ними. Для реалізації було обрано технологічний стек, такий як MERN (MongoDB, Express.js, React.js, Node.js) або LAMP (Linux, Apache, MySQL, PHP). Створено інтерфейс користувача, який дозволяє адміністраторам зручно додавати, редагувати та видаляти записи, а також переглядати звіти та статистику. Серверна частина обробляє запити користувачів та взаємодію з базою даних, реалізуючи маршрутизацію для управління різними типами запитів.

Особлива увага приділялася безпеці – були впроваджені механізми автентифікації та авторизації для обмеження доступу до адміністративних функцій та захисту даних. Після розгортання веб-застосунку на сервері проводилося його обслуговування, оновлення та усунення неполадок відповідно до потреб користувачів. Користувачам надавалися інструкції та навчання щодо роботи з застосунком для адміністрування даних. Такий підхід забезпечив створення ефективного веб-застосунку для управління даними системи рекомендацій, як показано на рисунках 5-6.

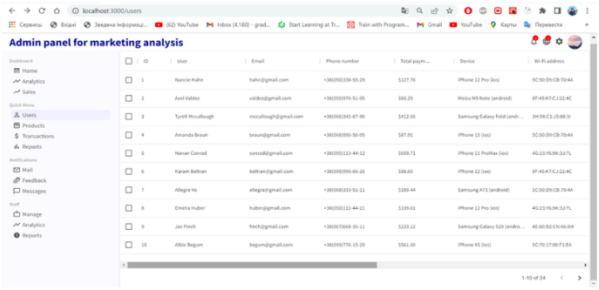

Рис. 5. Структура бази даних

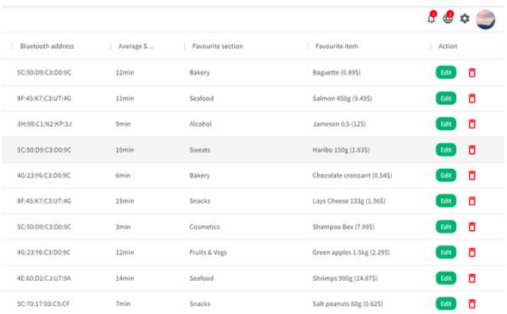

Рис. 6. Наповнення бази даних

Рисунки 7-8 ілюструють процес додавання, редагування та видалення записів у базі даних веб-застосунку для управління даними системи рекомендацій. Розробка веб-застосунку включала планування

користувацького інтерфейсу, вибір технологічного стеку (мови програмування, фреймворки, бази даних), реалізацію функціоналу для управління даними, забезпечення автентифікації та авторизації користувачів, а також створення компонентів як на стороні сервера, так і на стороні клієнта.

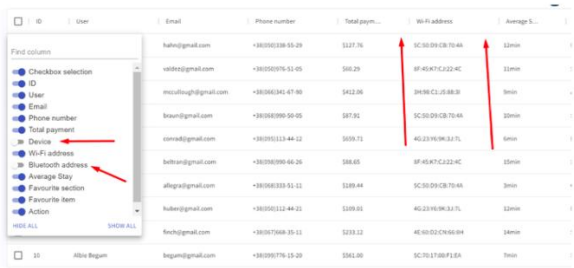

Рис. 7. Функції бази даних

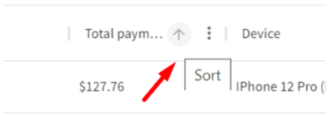

Рис. 8. Групування даних

Рис. 9 ілюструє функцію групування записів у веб-застосунку, яка дозволяє сортувати та організовувати дані за обраними параметрами для зручного перегляду та аналізу.

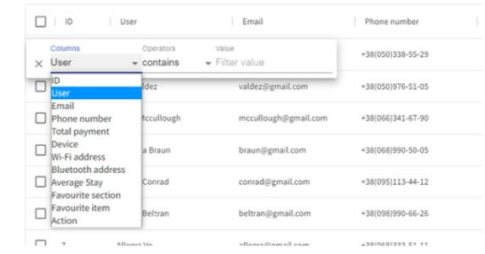

Рис. 9. Фільтрація бази даних

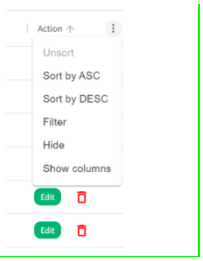

Рис. 10. Панель керування функціями

Рис. 11 показує панель функцій веб-застосунку для адміністрування даних, яка включає кнопки для редагування, видалення та інших інструментів управління записами.

Рис. 11. Аналітика веб-застосунку

Рис. 12 показує графічне відображення доходу магазину та відвідуваності за місяць на головній сторінці адмін-панелі веб-застосунку, що дозволяє оцінити тенденції продажів та ефективність бізнес-процесів.

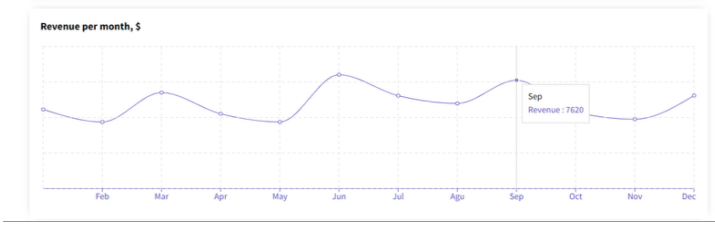

Рис. 12. Аналіз доходу

На основі аналізу існуючих IoT-рішень у сфері маркетингу, а також вивчення платформ та їх проблемних аспектів, була розроблена система, яка слугує інструментом підтримки для маркетологів і аналітиків. Система реалізована у вигляді адмін-панелі для відображення даних про клієнтів, отриманих за допомогою IoT-пристроїв.

Аналіз результатів показує, що реалізовані моделі та технології оцінювалися за точністю, ефективністю та застосовністю в реальних IoT-середовищах. Основні результати свідчать про те, що інтеграція показників компрометації (IoCs) суттєво покращує виявлення кіберзагроз, а моделі систем рекомендацій підвищують взаємодію користувачів і підтримку прийняття рішень у IoT-екосистемах. Порівняльний аналіз із існуючими підходами демонструє помітне поліпшення показників виявлення та часу реагування. З точки зору кібербезпеки використання IoCs дозволяє проактивно ідентифікувати та нейтралізувати загрози, зменшуючи потенційні втрати. Для IoT-застосувань моделі систем рекомендацій забезпечують інтелектуальну автоматизацію та персоналізовані сервіси, підвищуючи загальну зручність і ефективність системи. Для наукових досліджень поєднання механізмів безпеки на основі IoC із інтелектуальними моделями рекомендацій демонструє потенціал створення гібридних фреймворків.

Проте обмежені набори даних або симульовані середовища можуть не повністю відображати реальні сценарії атак. Масштабованість моделей та їх продуктивність при обробці великих потоків IoT-даних потребують додаткового тестування. Інтеграція з існуючими застарілими системами може створювати проблеми сумісності.

Поєднання технологій кібербезпеки на основі IoC із моделями систем рекомендацій для IoT-середовищ забезпечує значні переваги, включаючи підвищену здатність до виявлення загроз, покращену зручність користування системою та створює основу для подальших досліджень інтегрованих інтелектуальних систем.

ВИСНОВКИ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Було проведено аналіз наявних рішень у сферах Інтернету речей (IoT), маркетингу та аналітики даних, а також у суміжних галузях. Аналіз виявив нестачу доступних досліджень і підтвердив актуальність використання даних IoT для маркетингових цілей. Застосування цієї технології в маркетингу, особливо в роздрібній торгівлі, дозволяє отримувати цінні дані для автоматизації взаємодії з клієнтами, надання персоналізованих пропозицій у реальному часі та подальшої аналітичної обробки.

Було визначено та класифіковано ключові сценарії використання даних IoT-пристроїв для досягнення маркетингових цілей, а також систематизовано основні технології, придатні для реалізації цих сценаріїв та отримання релевантної аналітики. Аналіз існуючих IoT та маркетингових платформ показав, що жодна з них не надає комплексного рішення для маркетингових завдань; вони обмежуються кількома сценаріями, що перешкоджає повному використанню потенціалу IoT у маркетингу. Це підтвердило необхідність розробки систем, які інтегрують різні випадки використання IoT у маркетингові процеси.

Для впровадження такої системи було сформульовано вимоги за класифікацією FURPS+, розроблено архітектурні рекомендації для модуля обробки даних та спроектовано загальну архітектуру системи. Оскільки система взаємодіє з кількома платформами, було приділено увагу можливостям інтеграції з різними системами. З урахуванням необхідності вибору серед різних існуючих платформ та типів пристроїв проведено аналіз сучасних IoT-платформ, методів обробки даних та типів пристроїв, що дозволило сформувати практичні рекомендації щодо їх використання.

У майбутньому, оскільки об'єкт дослідження охоплює різні галузі та технології, сформульовані вимоги та рекомендації можуть бути доповнені та деталізовані, зокрема щодо вибору інтеграційних інструментів, протоколів, бібліотек, типів пристроїв та алгоритмів обробки, передачі та аналізу даних. На основі цих вимог можлива розробка повнофункціональної системи.

Крім того, було спроектовано та розроблено модуль виявлення руху, алгоритм якого може бути розгорнутий на фізичному пристрої. У поєднанні з іншими пристроями він формує IoT-систему для збору даних про клієнтів. Для візуалізації та аналізу зібраних даних створено веб-додаток, який допомагає аналітикам та маркетологам у розробці маркетингових стратегій.

Подальші дослідження можуть зосередитися на розширенні сценаріїв використання IoT у маркетингу, покращенні інтеграції з різними платформами та системами, оптимізації архітектури системи та алгоритмів обробки даних, а також на подальшому розвитку модулів збору, аналізу та візуалізації даних для створення повністю інтегрованої системи підтримки маркетингових рішень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Rahmati, M. (2025, February). *Federated learning driven cybersecurity framework for IoT networks with privacy preserving and real-time threat detection capabilities*. arXiv. https://arxiv.org/abs/2502.10599
2. Wu, J., Wang, Y., Dai, H., Xu, C., & Kent, K. B. (2023, March). *Adaptive bi-recommendation and self-improving network for heterogeneous domain adaptation assisted IoT intrusion detection*. arXiv. https://arxiv.org/abs/2303.14317
3. Lai, T., Farid, F., Bello, A., & Sabrina, F. (2023, July). *Ensemble learning-based anomaly detection for IoT cybersecurity via Bayesian hyperparameters sensitivity analysis*. arXiv. https://arxiv.org/abs/2307.10596
4. Mehedi, S. T., Anwar, A., Rahman, Z., Ahmed, K., & Islam, R. (2022, April). *Dependable intrusion detection system for IoT: A deep transfer learning-based approach*. arXiv. https://arxiv.org/abs/2204.04837
5. Haidur, H. I., Shulimova, D. D., Boyko, A. O., & Postnikov, Y. I. (2024). Model zabezpechennia kiberbezpeky Internetu rechei. *Telecommunication and Information Technologies*. https://tit.dut.edu.ua/index.php/telecommunication/article/view/2524
6. Zhydka, O. V., & Andriychenko, T. R. (2024). Informatsiina bezpeka system IoT. *Communication (Zhurnal)*. https://doi.org/10.31673/2412-9070.2024.046569
7. Merzlikin, Y., & Babeshko, Y. (2023). Analiz kiberbezpeky weboriientovanykh industrialnykh IoT-system. *ITSSI Journal, 24*. https://www.itssi-journal.com/index.php/ittsi/article/view/397
8. Dudykevych, V., Mykytyn, H., & Murak, T. (2025). Intehralna model bezpeky Internetu rechei u prostori intelektualizatsii obiektiv infrastruktury. *Cybersecurity: Education, Science, Technology*. https://csecurity.kubg.edu.ua/index.php/journal/article/view/848
9. Hlybovets, A., Shcherbyna, S., & Kiriienko, O. (2024). Vrazlyvosti bezpeky ta rishennia dlia zakhystu v systemakh Internetu rechei. *Naukovi zapysky NaUKMA*. https://doi.org/10.18523/2617-3808.2024.7.89-97
10. Zayats, V. (2024). Intehratsiia shtuchnoho intelektu v protokoly bezpeky Internetu rechei. *Kiberbezpeka ta kompiuterno intehrovani tekhnolohii*. https://conference.wunu.edu.ua/index.php/kbkit/article/view/733
11. Pedan, S. I., Melnyk, M. V., & Alekseyev, M. O. (2024). Pidvyshchennia bezpeky ziednannia IoT-prystroiv shliakhom analizu bezdrotovykh syhnaliv. In *Proceedings of the International Conference "Perspektyvy telekomunikatsii"*. https://conferenc-journal.its.kpi.ua/article/view/307418
12. Shabala, Y., & Korniichuk, B. (2024). Metodolohiia otsiniuvannia bezpeky IoT na promyslovykh obiektakh. *Upravlinnia rozvytkom skladnykh system*. https://doi.org/10.32347/2412-9933.2024.60.146-155
13. Klyap, M., Lyakh, I., Shumylo, N., & Tsipinyo, A. (2025). Bezpeka IoT protokoliv yak vyklyk dlia mizhnarodnoho spivrobitnytstva. *Nauka i tekhnika sohodni*. https://dspace.uzhnu.edu.ua/items/2dfa3e55-9e32-4e78-a328-5c5c5a502c3f
14. Pavlenko, K. Y., & Sribna, I. M. (2025). *Modeliuvannia zahroz bezpetsi v IoT systemakh okhorony: Pidkhody do minimizatsii ryzykiv* (Master's thesis). https://conf.ztu.edu.ua/wp-content/uploads/2025/01/103.pdf
15. Shabala, Y. (2025). *Model hibrydnoi IoT systemy z pidvyshchenym rivnem informatsiinoi bezpeky* (Qualification work). https://ir.library.knu.ua/entities/publication/c6919d27-5039-4948-857f-f0463f305ae1

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023

Nataliia Cherniiashchuk
Doctor of Pedagogical Sciences, Professor
Lesya Ukrainka Volyn National University, Lutsk, Ukraine
ORCID: 0000-0002-3178-8377
cherniashchuk.nataliia@vnu.edu.ua

ADAPTIVE RECOMMENDATION MODEL FOR CYBERSECURITY MANAGEMENT IN IOT ENVIRONMENTS

Abstract. Recommendation systems for decision support in Internet of Things (IoT) environments play a key role in the development of effective intelligent solutions, providing adaptive cybersecurity management and resource optimization for IoT platforms. Special attention is given to the characteristics of IoT data, which are generated from numerous sources such as sensors, communication devices, and other infrastructure elements, resulting in large volumes of heterogeneous data. This study investigates modern recommendation methods, including collaborative filtering, content-based approaches, deep neural networks, and ensemble learning, as well as their effectiveness in real-world IoT environments. Particular focus is placed on challenges related to algorithm scalability, performance, and energy optimization in low-power devices.

The aim of this research is to develop an adaptive recommendation model to support decision-making in IoT environments with a high level of cybersecurity. To achieve this, the study analyzes recent scientific research and solutions in the field of IoT and recommendation systems, examines contemporary platforms implementing similar approaches, identifies technologies and methods suitable for building a recommendation system, and develops a personalized decision support model. The work presents the integration of machine learning methods, big data analytics, and intelligent information processing to ensure adaptive responses to cyber threats.

The results demonstrate the potential of combining indicators of compromise, intelligent recommendation models, and threat prediction algorithms to enhance the security of IoT ecosystems. The proposed model not only improves threat detection and real-time response but also enables intelligent management processes, automation of operations, and personalized decision support for IoT system administrators and users. The study highlights the scientific and practical significance of integrating adaptive recommendations into IoT cybersecurity, providing a foundation for further development of hybrid solutions utilizing artificial intelligence and big data processing methods.

Keywords: IoT (Internet of Things), recommendation system, personalized recommendations, IoT ecosystem, data processing, machine learning, big data analytics, decision-making, intelligent systems, sensor data.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Rahmati, M. (2025, February). *Federated learning driven cybersecurity framework for IoT networks with privacy-preserving and real-time threat detection capabilities*. arXiv. https://arxiv.org/abs/2502.10599
2. Wu, J., Wang, Y., Dai, H., Xu, C., & Kent, K. B. (2023, March). *Adaptive bi-recommendation and self-improving network for heterogeneous domain adaptation assisted IoT intrusion detection*. arXiv. https://arxiv.org/abs/2303.14317
3. Lai, T., Farid, F., Bello, A., & Sabrina, F. (2023, July). *Ensemble learning-based anomaly detection for IoT cybersecurity via Bayesian hyperparameters sensitivity analysis*. arXiv. https://arxiv.org/abs/2307.10596
4. Mehedi, S. T., Anwar, A., Rahman, Z., Ahmed, K., & Islam, R. (2022, April). *Dependable intrusion detection system for IoT: A deep transfer learning-based approach*. arXiv. https://arxiv.org/abs/2204.04837
5. Haidur, H. I., Shulimova, D. D., Boyko, A. O., & Postnikov, Y. I. (2024). Model zabezpechennia kiberbezpeky Internetu rechei. *Telecommunication and Information Technologies*. https://tit.dut.edu.ua/index.php/telecommunication/article/view/2524
6. Zhydka, O. V., & Andriychenko, T. R. (2024). Informatsiina bezpeka system IoT. *Communication (Zhurnal)*. https://doi.org/10.31673/2412-9070.2024.046569

7. Merzlikin, Y., & Babeshko, Y. (2023). Analiz kiberbezpeky weboriientovanykh industrialnykh IoT-system. *ITSSI Journal*, *24*. https://www.itssi-journal.com/index.php/ittsi/article/view/397
8. Dudykevych, V., Mykytyn, H., & Murak, T. (2025). Intehralna model bezpeky Internetu rechei u prostori intelektualizatsii obiektiv infrastruktury. *Cybersecurity: Education, Science, Technology*. https://csecurity.kubg.edu.ua/index.php/journal/article/view/848
9. Hlybovets, A., Shcherbyna, S., & Kiriienko, O. (2024). Vrazlyvosti bezpeky ta rishennia dlia zakhystu v systemakh Internetu rechei. *Naukovi zapysky NaUKMA*. https://doi.org/10.18523/2617-3808.2024.7.89-97
10. Zayats, V. (2024). Intehratsiia shtuchnoho intelektu v protokoly bezpeky Internetu rechei. *Kiberbezpeka ta kompiuterno intehrovani tekhnolohii*. https://conference.wunu.edu.ua/index.php/kbkit/article/view/733
11. Pedan, S. I., Melnyk, M. V., & Alekseyev, M. O. (2024). Pidvyshchennia bezpeky ziednannia IoT-prystroiv shliakhom analizu bezdrotovykh syhnaliv. In *Proceedings of the International Conference "Perspektyvy telekomunikatsii"*. https://conferenc-journal.its.kpi.ua/article/view/307418
12. Shabala, Y., & Korniichuk, B. (2024). Metodolohiia otsiniuvannia bezpeky IoT na promyslovykh obiektakh. *Upravlinnia rozvytkom skladnykh system*. https://doi.org/10.32347/2412-9933.2024.60.146-155
13. Klyap, M., Lyakh, I., Shumylo, N., & Tsipinyo, A. (2025). Bezpeka IoT protokoliv yak vyklyk dlia mizhnarodnoho spivrobitnytstva. *Nauka i tekhnika sohodni*. https://dspace.uzhnu.edu.ua/items/2dfa3e55-9e32-4e78-a328-5c5c5a502c3f
14. Pavlenko, K. Y., & Sribna, I. M. (2025). *Modeliuvannia zahroz bezpetsi v IoT systemakh okhorony: Pidkhody do minimizatsii ryzykiv* (Master's thesis). https://conf.ztu.edu.ua/wp-content/uploads/2025/01/103.pdf
15. Shabala, Y. (2025). *Model hibrydnoi IoT systemy z pidvyshchenym rivnem informatsiinoi bezpeky* (Qualification work). https://ir.library.knu.ua/entities/publication/c6919d27-5039-4948-857f-f0463f305ae1

Отримано редакцією журналу / Received: 25.11.25
Прорецензовано / Revised: 14.01.26
Схвалено до друку / Accepted: 25.06.26