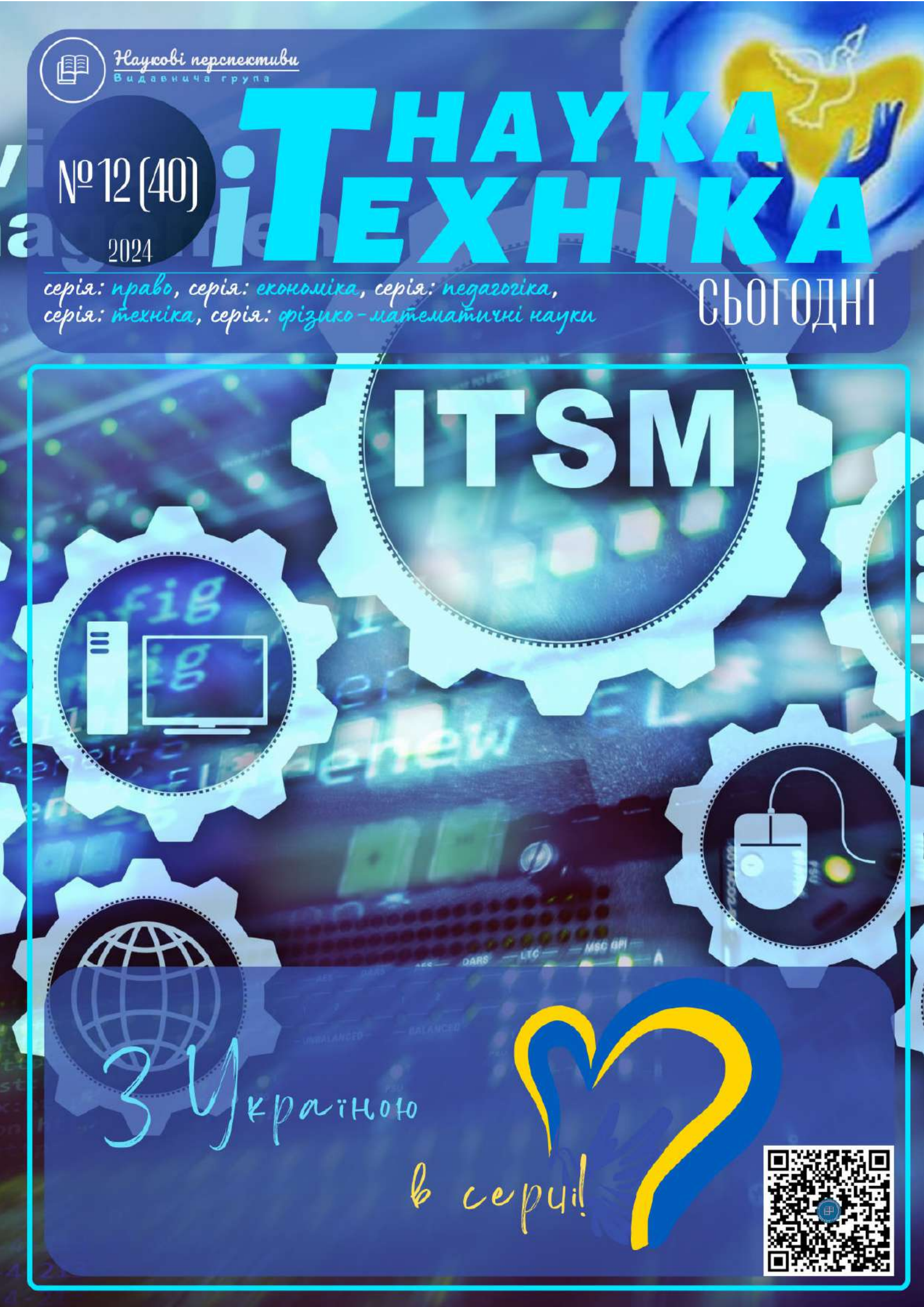
Наукові перспективи
Видавнича група

НАУКА і ТЕХНІКА СЬОГОДНІ

№ 12 (40)
2024

серія: право, серія: економіка, серія: педагогіка,
серія: техніка, серія: фізико-математичні науки



Видавнича група «Наукові перспективи»

Всеукраїнська Асамблея докторів наук із державного управління

Асоціація науковців України

«Наука і техніка сьогодні»

(Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»)

Випуск № 12(40) 2024

Київ – 2024

Publishing Group «Scientific Perspectives»

Ukrainian Assembly of Doctors of Sciences in Public Administration

Association of Scientists of Ukraine

"Science and technology today"

("Pedagogy" series, "Law" series, "Economics" series, "Physical and mathematical sciences" series, "Technics" series)

Issue № 12(40) 2024

Kyiv – 2024

ISSN 2786-6025 Online
УДК 001.32:1 /3](477)(02)

DOI: https://doi.org/10.52058/2786-6025-2024-12(40)

«Наука і техніка сьогодні» (Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»)»: журнал. 2024. № 12(40) 2024. С. 1637

Згідно наказу Міністерства освіти і науки України від 07.04.2022 № 320 журналу присвоєно категорію "Б" із економіки та педагогіки (спеціальності – 015 - Педагогічні науки; 076 - Економічні науки)

Згідно наказу Міністерства освіти і науки України від 06.06.2022 № 530 журналу присвоєно категорію "Б" із права (спеціальність – 081 Юридичні науки)

Згідно наказу Міністерства освіти і науки України від 10.10.2022 № 894 журналу присвоєно категорію "Б" із техніки (спеціальність - 122 Комп'ютерні науки)

Журнал видається за підтримки Міждержавної гільдії інженерів консультантів, Інституту філософії та соціології Національної Академії Наук Азербайджану (Баку, Азербайджан), громадської організації «Християнська академія педагогічних наук України» та громадської організації «Всеукраїнська асоціація педагогів і психологів з духовно-морального виховання»

Рекомендовано до видавництва Президією Всеукраїнської Асамблеї докторів наук з державного управління (Рішення від 25.11.2024, № 18/11-24)

Журнал включено до міжнародної наукометричної бази Index Copernicus (IC), міжнародної пошукової системи Google Scholar та до міжнародної наукометричної бази даних Research Bible

№ 12(40)
2024
НАУКА і ТЕХНІКА СЬОГОДНІ
серії: право, економіка, педагогіка, техніка, фізико-математичні науки

ЗМІСТ

СЕРІЯ «Право»

Korshun A.V. 19
SIGNATURES AND SHORT HANDWRITING RECORDS MADE WITH THE HELP OF TECHNICAL TECHNIQUES AS AN OBJECT OF A COMPREHENSIVE FORENSIC INVESTIGATION

Балакарєва І.М., Діденко В.Ю. 30
ПОЗБАВЛЕННЯ ПРАВА НА ОТРИМАННЯ ОДНОРАЗОВОЇ ГРОШОВОЇ ДОПОМОГИ У ЗВ'ЯЗКУ З ЗАГИБЕЛЛЮ (СМЕРТЮ) ВІЙСЬКОВОСЛУЖБОВЦЯ: ЕВОЛЮЦІЯ ПРАВА І ЙОГО ЗАСТОСУВАННЯ

Бєлікова М.І. 44
ШТУЧНИЙ ІНТЕЛЕКТ В АДМІНІСТРАТИВНОМУ СУДОЧИНСТВІ

Гавриленко В.В. 53
РОЛЬ МІЖНАРОДНО-ПРАВОВИХ СТАНДАРТІВ У ВИРІШЕННІ ПРОБЛЕМ РЕФОРМУВАННЯ СУДОВОЇ СИСТЕМИ УКРАЇНИ

Зільник Н.М., Яровик Д.Р. 66
АВТОРСЬКІ ПРАВА В ЕПОХУ СОЦІАЛЬНИХ МЕРЕЖ: ПРОБЛЕМИ ТА МОЖЛИВОСТІ РЕГУЛЮВАННЯ

Кулик С.В. 80
ІМПЛЕМЕНТАЦІЯ МІЖНАРОДНО-ПРАВОВИХ СТАНДАРТІВ У НАЦІОНАЛЬНІ СУДОВІ СИСТЕМИ ЗА ПОГЛЯДАМИ ЗАКОРДОННИХ НАУКОВЦІВ

Лопоха В.В., Чайка Р.А. 93
ЮРИДИЧНА ПРИРОДА СУДОВОЇ ЕКСПЕРТИЗИ: СУЧАСНІ ПІДХОДИ ТА ТЕОРЕТИЧНІ ДИСКУСІЇ

Медвідь А.Б., Медвідь Ю.О. 108
ПРАВО НА ДОСТУП ДО СУДУ ЯК ОБОВ'ЯЗКОВИЙ СТРУКТУРНИЙ ЕЛЕМЕНТ ПРАВА НА СПРАВЕДЛИВИЙ СУД

Мельник О.П., Полюхович І.І., Сторожук А.О. 118
ВПЛИВ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ НА ПОДАТКОВЕ АДМІНІСТРУВАННЯ

Меренич О.С. 126
ВЕКТОРИ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Олійник У.М. 133
ОСОБЛИВОСТІ ПРАЦЕВЛАШТУВАННЯ ПРАЦІВНИКІВ В УМОВАХ ВОЄННОГО СТАНУ

Падалко О.О. 143
«ЩОДО ПИТАННЯ ПРИПИНЕННЯ ТРУДОВИХ ПРАВОВІДНОСИН В УМОВАХ ВОЄННОГО СТАНУ»

Слободенюк І.В. 157
СУДОВИЙ КОНТРОЛЬ ЗА ДІЯМИ ТА РІШЕННЯМИ ДІЗНАВАЧА У КРИМІНАЛЬНОМУ ПРОЦЕСІ

Христова Ю.В. 168
АКТУАЛЬНІ ПИТАННЯ ПРОТИДІЇ КРИМІНОГЕННИМ ВПЛИВАМ НА БЕЗПЕКУ ПРАВОСУДДЯ НАЦІОНАЛЬНОЮ ПОЛІЦІЄЮ В УМОВАХ ВОЄННОГО СТАНУ

Цимбалюк В.І. 180
ЗАБЕЗПЕЧЕННЯ СЛІДЧИМ СУДДЕЮ ПРАВ ПОТЕРПІЛОГО ПІД ЧАС ДОСУДОВОГО РОЗСЛІДУВАННЯ

Юрко В.В. 191
СУЧАСНИЙ СТАН ДОСЛІДЖЕННЯ ЦИВІЛЬНО-ПРАВОВИХ СПОСОБІВ ЗАХИСТУ ПРАВ СПОЖИВАЧІВ

СЕРІЯ «Економіка»

Гавран В.Я., Комар Ю.О., Грибик І.І. 200
СУЧАСНІ СТРАТЕГІЇ ТА ІНСТРУМЕНТИ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ПІДПРИЄМСТВ ТОРГІВЛІ

Гевчук А.В., Лисяний М.П. 210
ВДОСКОНАЛЕННЯ ОБЛІКОВО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ВИКОНАНИХ ПОСЛУГ ЧЕРЕЗ ЗАСТОСУВАННЯ ПРОГРАМНОГО ПРОДУКТУ MASTER-БУХГАЛТЕРІЯ

Гончар С.Й. 223
ІНВЕСТИЦІЇ У РОЗВИТОК ЛЮДСЬКОГО КАПІТАЛУ В КОНТЕКСТІ ПІДВИЩЕННЯ РІВНЯ КАДРОВОЇ БЕЗПЕКИ

Іваненко В.Ф., Іваненко Ф.В. 234
ФОРМУВАННЯ ПОПИТУ ТА ЕФЕКТИВНІСТЬ ВИРОЩУВАННЯ ЯГІД ГОДЖІ

Коляджин І.Ф., Коциловський Б.А., Гуцуляк М.І., Коляджин Ю.І. 247
ОСОБЛИВОСТІ ВЕДЕННЯ ЛІСОВОГО ГОСПОДАРСТВА У СМЕРЕКОВИХ НАСАДЖЕННЯХ В СУЧАСНИХ УМОВАХ ГІРСЬКОГО ЛІСІВНИЦТВА

Лісовська Л.С., Бас І.О. 255
ІНТЕГРОВАНИЙ ПІДХІД В УПРАВЛІННІ ІННОВАЦІЙНИМИ ПРОЦЕСАМИ ПІДПРИЄМСТВ: ОГЛЯД СУЧАСНИХ АКАДЕМІЧНИХ ДОСЛІДЖЕНЬ

Михаліцька Н.Я., Яцик М.Р. 267
ЛІДЕРСТВО В СИСТЕМІ СТРАТЕГІЧНОГО УПРАВЛІННЯ БІЗНЕС-ОРГАНІЗАЦІЄЮ В УМОВАХ СУЧАСНОЇ КРИЗИ

Москвяк Я.Є. 277
ТЕОРЕТИЧНІ АСПЕКТИ ФІНАНСОВОГО ПЛАНУВАННЯ ТА ПРОГНОЗУВАННЯ В ПІДПРИЄМСТВІ

Правдюк М.В. 286
ВПЛИВ СОЦІАЛЬНИХ МЕРЕЖ НА ЕФЕКТИВНІСТЬ ТА ВЕДЕННЯ БІЗНЕСУ

Правдюк М.В. 302
CASHBACK ЯК ЕЛЕМЕНТ РОЗВИТКУ МАЛОГО БІЗНЕСУ

Рачковський Е.А. 315
ТЕНДЕНЦІЇ РОЗВИТКУ ТРАНСПОРТНОЇ ГАЛУЗІ: ГЛОБАЛЬНІ ВИКЛИКИ ТА ПЕРСПЕКТИВИ ДЛЯ УКРАЇНИ

Снігова О.Ю., Ципліцька О.О. 328
ТЕОРЕТИЧНІ ЗАСАДИ ПРОСТОРОВОГО РОЗВИТКУ ПРОМИСЛОВОСТІ

Угоднікова О.І., Виноградов В.В., Пигида Д.А. 345
ВИБІР КОНКУРЕНТНИХ МАРКЕТИНГОВИХ СТРАТЕГІЙ СОЦІАЛЬНО-ЕКОНОМІЧНОГО РОЗВИТКУ

Щитов Д.М., Мормуль М.Ф. 354
РОЛЬ ТА ФУНКЦІЇ КРИПТОВАЛЮТИ В ЕЛЕКТРОННІЙ КОМЕРЦІЇ

СЕРІЯ «Педагогіка»

Akimova O.V., Sapohov M.V., Hapchuk Y.A., Salii R.V. 369
LEADERSHIP QUALITIES IN EDUCATIONAL MANAGEMENT

Diachenko M.O. 381
THE PROBLEM OF DEVELOPING THE PROFESSIONAL THINKING OF THE FUTURE HISTORY TEACHER IN THE CONTEXT OF EUROPEAN INTEGRATION PROCESSES

Антонів Р.Р. 393
ІНКЛЮЗИВНА КОМПЕТЕНТНІСТЬ ЯК ЧИННИК ПРОФЕСІЙНОГО СТАНОВЛЕННЯ ФАХІВЦІВ У СИСТЕМІ ВИЩОЇ МЕДИЧНОЇ ОСВІТИ

Балакірєва В.А. 404
ОСОБЛИВОСТІ ВПРОВАДЖЕННЯ STEM-ТЕХНОЛОГІЇ У ПРОЦЕС НАВЧАННЯ ПРИРОДОЗНАВСТВА В ПОЧАТКОВІЙ ШКОЛІ

Берегова Г.Д., Фролова М.Е., Момоток О.М. 415
РОЛЬ ОСВІТНІХ УСТАНОВ У ПРОФЕСІЙНОМУ САМОВИЗНАЧЕННІ СТУДЕНТІВ В СУЧАСНИХ УМОВАХ

Білавич Г.В., Вінтоняк О.В., Дідух І.Я., Вербещук С.В. 426
МУЗЕЙНА ПЕДАГОГІКА КРІЗЬ ПРИЗМУ ПРОФЕСІЙНОЇ ПІДГОТОВКИ МАЙБУТНІХ ФАХІВЦІВ У СИСТЕМІ ПЕРЕДВИЩОЇ ТА ВИЩОЇ ОСВІТИ

Богів Е.І., Когуч М.В. 438
СОЦІАЛІЗАЦІЯ ПІДЛІТКІВ ТА ВПЛИВ НА ЦЕЙ ПРОЦЕС РЕАЛІЙ ТА ВИКЛИКІВ СЬОГОДЕННЯ

Бойченко В.В., Тіщенко А.В. 450
ПРОБЛЕМА ФОРМУВАННЯ НАЦІОНАЛЬНОЇ ТА ГРОМАДЯНСЬКОЇ ІДЕНТИЧНОСТІ ПІДРОСТАЮЧОГО ПОКОЛІННЯ

Бурчак С.О., Капаєв В.В. 462
ЦІЛІ ФОРМУВАННЯ ПРОФЕСІЙНОЇ КОМПЕТЕНТНОСТІ МАЙБУТНІХ ПЕДАГОГІВ ПРОФЕСІЙНОГО НАВЧАННЯ В ПЕДАГОГІЧНИХ ЗАКЛАДАХ ВИЩОЇ ОСВІТИ

Бялик О.В. 472
ФОРМУВАННЯ ГЕНДЕРНОЇ КОМПЕТЕНТНОСТІ ЗДОБУВАЧІВ ОСВІТИ: ПОГЛЯД НА ПРОБЛЕМУ

Варнавська І.В. 482
ПІДВИЩЕННЯ МОТИВАЦІЇ ДО НАВЧАННЯ ЧЕРЕЗ АКТИВНІСТЬ В УМОВАХ ВІЙНИ НА ПРИКЛАДІ ЗДОБУВАЧІВ ХЕРСОНСЬКОГО ДЕРЖАВНОГО АГРАРНО-ЕКОНОМІЧНОГО УНІВЕРСИТЕТУ

Васютіна Т.М. 491
РОЛЬ ФОРМАЛЬНОЇ ТА НЕФОРМАЛЬНОЇ ОСВІТИ У ПІДГОТОВЦІ МАЙБУТНІХ УЧИТЕЛІВ ДО РОБОТИ В ІНКЛЮЗИВНОМУ ОСВІТНЬОМУ СЕРЕДОВИЩІ

Веремюк Л.Л., Авчіннікова Г.Д. 501
МЕТОДИЧНІ ПІДХОДИ У ВИКЛАДАННІ ГРАМАТИКИ НІМЕЦЬКОЇ МОВИ

Вовчаста Н.Я., Шемелюк Г.О., Білик О.С., Волошин М.М. 512
КОНЦЕПТУАЛЬНІ ЗАСАДИ НАВЧАННЯ СТУДЕНТІВ ОСНОВ МОДЕЛЮВАННЯ ЯК ЗАСОБУ ПІДВИЩЕННЯ РЕЗУЛЬТАТИВНОСТІ ПРОФЕСІЙНОЇ ПІДГОТОВКИ

Глазова В.В. 523
ІНТЕГРАЦІЯ ЕЛЕМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ В МЕТОДИКУ НАВЧАННЯ ІНФОРМАТИКИ

Гордієнко Ю.А. 536
ОРГАНІЗАЦІЙНО-ПЕДАГОГІЧНІ УМОВИ ФОРМУВАННЯ ІНШОМОВНОЇ КОМУНІКАТИВНО-МОВЛЕННЄВОЇ КОМПЕТЕНТНОСТІ МАЙБУТНІХ УЧИТЕЛІВ ІНОЗЕМНИХ МОВ

Гриньова М.В., Титаренко О.О. 547
КРИТЕРІЇ ОЦІНЮВАННЯ РІВНЯ ГОТОВНОСТІ СТУДЕНТІВ ДО НАУКОВО-ДОСЛІДНИЦЬКОЇ ДІЯЛЬНОСТІ

Гулько Т.Ю. 559
ФОРМУВАННЯ ЗДОРОВ'ЯЗБЕРЕЖУВАЛЬНОЇ КОМПЕТЕТНОСТІ У МАЙБУТНІХ ФАХІВЦІВ ФІЗИЧНОЇ КУЛЬТУРИ ТА СПОРТУ ЯК ПЕДАГОГІЧНА І СОЦІАЛЬНА ПРОБЛЕМА

Десятник К.В. 575
ЛІДЕРСЬКА КОМПЕТЕНТНІСТЬ МАЙБУТНЬОГО ВЧИТЕЛЯ ПОЧАТКОВОЇ ШКОЛИ: НАУКОВІ ПІДХОДИ ДО РОЗУМІННЯ СУТНОСТІ ПОНЯТТЯ

Димовська А.К. 588
ПОТЕНЦІАЛ МЕТОДУ ПОВІЛЬНОГО ЧИТАННЯ (CLOSE READING) У СУЧАСНІЙ ЛІТЕРАТУРНІЙ ОСВІТІ УЧНІВ ПОЧАТКОВОЇ ШКОЛИ

Дядечко І.Є., Верітов О.І. 599
СУЧАСНІ ТЕХНОЛОГІЇ В СПОРТІ ЯК СКЛАДОВА ОСВІТНЬОГО ПРОЦЕСУ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Захаревич М. 607
МЕТОДИКА CLIL В КОНТЕКСТІ ІНТЕГРОВАНОГО ПІДХОДУ У ВИВЧЕННІ ІНОЗЕМНОЇ МОВИ

Зорочкіна Т. С., Гнезділова К.М., Степанова Н.М. 642
ПІДГОТОВКА МАЙБУТНІХ УЧИТЕЛІВ ПОЧАТКОВОЇ ШКОЛИ ДО ВИКОРИСТАННЯ ЦИФРОВИХ ОСВІТНІХ ТЕХНОЛОГІЙ У ПРОФЕСІЙНІЙ ДІЯЛЬНОСТІ

Іванюк Г.І. 651
ОСОБИСТІСНИЙ ТА ПРОФЕСІЙНИЙ КОНТЕКСТИ ПІДГОТОВКИ МАГІСТРІВ ДО ДОСЛІДНИЦТВА В СФЕРІ ОСВІТИ

Калько Д.Р., Січко Т.В., Сеник І.О. 665
ШТУЧНИЙ ІНТЕЛЕКТ В ОПТИМІЗАЦІЇ ОСВІТНЬОГО ПРОЦЕСУ: ПІДХОДИ ТА МЕТОДИ

Котило А.О. 678
ПСИХОЛОГІЧНІ ТА ВІКОВІ АСПЕКТИ ЗАСВОЄННЯ АНГЛІЙСЬКОЇ МОВИ УЧНЯМИ МОЛОДШИХ КЛАСІВ У КОНТЕКСТІ НУШ

Куліненко Л.Б., Яренчук Л.Г. 685
РОЗВИТОК ПІЗНАВАЛЬНОГО ІНТЕРЕСУ УЧНІВ ДО ВИВЧЕННЯ ФІЗИКИ В РАМКАХ ПОЗАУРОЧНОЇ ДІЯЛЬНОСТІ: АНАЛІЗ СТАНУ ПРОБЛЕМИ

Литвинська Т.Ю. 694
ОСОБЛИВОСТІ ПЕРЕКЛАДУ ВІЙСЬКОВОЇ ТЕРМІНОЛОГІЇ

Лоюк О.В. 703
ДІАГНОСТИЧНИЙ ІНСТРУМЕНТАРІЙ ДЛЯ ВСТАНОВЛЕННЯ РІВНІВ СФОРМОВАНОСТІ НАВИЧОК ПРОЄКТУВАННЯ У МОЛОДШИХ ШКОЛЯРІВ

Мкртічян О.А., Андрощук І.П., Фоміна Л.В., Дмитрієва Н.Б., Лунгу К.В. 718
ІННОВАЦІЙНІ ПІДХОДИ ДО ВИКЛАДАННЯ ПРОФЕСІЙНО-ОРІЄНТОВАНИХ ДИСЦИПЛІН У ВИЩІЙ ОСВІТІ: АНАЛІЗ СУЧАСНИХ МЕТОДИК

Пак А., Юмрукуз А.А., Хон К.Ю. 733
ПРОБЛЕМИ КОГНІТИВНОЇ ЛІНГВІСТИКИ В ВИКЛАДАННІ КОРЕЙСЬКОЇ МОВИ

Перфільєва Л.П. 743
ІННОВАЦІЙНІСТЬ У ПІДГОТОВЦІ МАЙБУТНІХ ВЧИТЕЛІВ ПОЧАТКОВИХ КЛАСІВ ПРИ ВИКЛАДАННІ ПРЕДМЕТІВ ПРИРОДНИЧОЇ ОСВІТНЬОЇ ГАЛУЗІ

Подолянчук С.В. 751
ВИВЧЕННЯ ОСОБЛИВОСТЕЙ РОЗРАХУНКУ НА СТИСКАННЯ ПІД ЧАС ПІДГОТОВКИ УЧИТЕЛІВ ТРУДОВОГО НАВЧАННЯ ТА ТЕХНОЛОГІЙ

Пономаренко Л.П. 761
МЕТОДОЛОГІЯ ВИКОРИСТАННЯ BIG DATA У ФІЗИЧНИХ ДОСЛІДЖЕННЯХ: ПІДХОДИ ТА ПЕРСПЕКТИВИ ДЛЯ СТУДЕНТІВ-ФІЗИКІВ

Поручинський В.І., Куцевич А.М. 778
ЗАСОБИ ТА ІНСТРУМЕНТИ ДЛЯ ОРГАНІЗАЦІЇ ДИСТАНЦІЙНОГО НАВЧАННЯ В ЗАКЛАДАХ ЗАГАЛЬНОЇ СЕРЕДНЬОЇ ОСВІТИ

Радзівіл Т.А., Бай Ю.М., Хижко О.В. 787
КЕЙС-ТЕХНОЛОГІЇ В ОСВІТНЬОМУ ПРОЦЕСІ ПІДГОТОВКИ ІНСТРУМЕНТАЛІСТІВ У ЗАКЛАДАХ ВИЩОЇ ОСВІТИ

Рожкова М.Г. 797
ЦИФРОВА ТРАНСФОРМАЦІЯ ЯК ФАКТОР УДОСКОНАЛЕННЯ МЕТОДІВ ВИКЛАДАННЯ ІНОЗЕМНИХ МОВ У ВИЩІЙ ШКОЛІ

Росенко Д.О. 807
ВПЛИВ ФІЗИЧНОЇ АКТИВНОСТІ НА ВІДНОВЛЕННЯ МЕНТАЛЬНОГО ЗДОРОВ'Я ЛЮДИНИ

Руденко А.В. 816
МІЖНАРОДНІ СТАНДАРТИ І РЕКОМЕНДАЦІЇ ЩОДО ПРОФЕСІЙНОЇ ПІДГОТОВКИ МАЙБУТНІХ БАКАЛАВРІВ З ГЕОГРАФІЇ

Савенко Л.П. 826
ФОРМУВАННЯ ПРОФЕСІЙНОЇ МОВНО-КОМУНІКАТИВНОЇ КОМПЕТЕНТНОСТІ СТУДЕНТІВ ПРИ ВИКЛАДАННІ ДИСЦИПЛІНИ «УКРАЇНСЬКА МОВА ЗА ПРОФЕСІЙНИМ СПРЯМУВАННЯМ»

Силадій І.М., Кучай Т.П., Дутка Г.Я. 838
ФОРМУВАННЯ ГОТОВНОСТІ МАЙБУТНІХ ПЕДАГОГІВ ДО УПРАВЛІННЯ ОСВІТНЬОЮ ДІЯЛЬНІСТЮ ЗДОБУВАЧІВ ОСВІТИ

Смолянко Ю.М., Гарус К.М. 844
ОСОБЛИВОСТІ ФОРМУВАННЯ ЕМОЦІЙНОЇ КУЛЬТУРИ ДИТИНИ СТАРШОГО ДОШКІЛЬНОГО ВІКУ ЗАСОБАМИ КАЗОК

Спольська О.В., Ванюга Л.С., Небесна Ю.В. 856
ТРЕНІНГИ З АКТОРСЬКОЇ МАЙСТЕРНОСТІ ЯК ЗАСІБ РОЗВИТКУ ПРОФЕСІЙНИХ КОМПЕТЕНЦІЙ: ПОРІВНЯЛЬНИЙ АНАЛІЗ КЛАСИЧНИХ ТА ІННОВАЦІЙНИХ ПІДХОДІВ

Сухопара І.Г., Згонник В.А. 866
ПОТЕНЦІАЛ УКРАЇНСЬКОЇ НАРОДНОЇ ГРИ У ВИВЧЕННІ ГРОМАДЯНСЬКОЇ ТА ІСТОРИЧНОЇ ОСВІТНЬОЇ ГАЛУЗІ В ПОЧАТКОВІЙ ШКОЛІ

Ткачова Н.О., Лимаренко О.А. 878
МІЖКУЛЬТУРНА ВЗАЄМОДІЯ У ПРОФЕСІЙНІЙ ДІЯЛЬНОСТІ БАКАЛАВРА ФІЛОЛОГІЇ: ЦІННІСНІ АСПЕКТИ ТА ПРАКТИЧНА РЕАЛІЗАЦІЯ

Хон К.Ю. 886
ВПРОВАДЖЕННЯ КОМУНІКАТИВНОГО ПІДХОДУ ЯК ЗАСОБУ РОЗВИТКУ МОВЛЕННЄВИХ ЗДІБНОСТЕЙ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ ПЕРШОГО (БАКАЛАВРСЬКОГО) РІВНЯ В ПРОЦЕСІ ВИВЧЕННЯ КОРЕЙСЬКОЇ МОВИ

Цецик С.П., Цецик Я.П. 895
ФОРМУВАННЯ ГРОМАДЯНСЬКОЇ КОМПЕТЕНЦІЇ ЗДОБУВАЧІВ ПІД ЧАС НАВЧАННЯ СУСПІЛЬНИХ ДИСЦИПЛІН

Цуканова А.О., Дерученко В.С. 904
ІСТОРИЧНІ «РОДЗИНКИ» НА ЗАНЯТТЯХ ІЗ ВИЩОЇ МАТЕМАТИКИ (НА ПРИКЛАДІ ПРАКТИЧНОГО ЗАНЯТТЯ З ТЕМИ «ЗБІЖНІСТЬ ЧИСЛОВИХ РЯДІВ»)

Цуканова А.О., Дерученко В.С. 917
ІСТОРИЧНИЙ МАТЕРІАЛ НА ЗАНЯТТЯХ ІЗ ВИЩОЇ МАТЕМАТИКИ (НА ПРИКЛАДІ ПОЄДНАННЯ НА ПРАКТИЧНОМУ ЗАНЯТТІ З ОПЕРАЦІЙНОГО ЧИСЛЕННЯ ДВОХ ТЕМ: «ЗНАХОДЖЕННЯ ЗОБРАЖЕНЬ ЗА ДОПОМОГОЮ ПЕРЕТВОРЕННЯ ЛАПЛАСА», «ІСТОРІЯ П'ЄР СІМОНА ЛАПЛАСА – РІЗНОБІЧНО АПОЛІТИЧНОГО ГОРДІВНИКА ТА НАЙВІРНІШОГО ПРИХИЛЬНИКА «НЕСКІНЧЕННО МАЛИХ»)

Цуканова А.О., Дерученко В.С. 942
ЕКСКУРС В ІСТОРІЮ НА ЗАНЯТТЯХ ІЗ ВИЩОЇ МАТЕМАТИКИ (НА ПРИКЛАДІ ПОЄДНАННЯ НА ПРАКТИЧНОМУ ЗАНЯТТІ З ДИФЕРЕНЦІАЛЬНИХ РІВНЯНЬ ДВОХ ТЕМ: «РОЗВ'ЯЗУВАННЯ РІВНЯНЬ ПЕРШОГО ПОРЯДКУ МЕТОДОМ ЛАГРАНЖА», «ІСТОРІЯ ЖОЗЕФ ЛУЇ ЛАГРАНЖА – НАЙСКРОМНІШОГО МАТЕМАТИКА XVIII СТОЛІТТЯ»)

Цуканова А.О. 967
ІСТОРИЗМИ НА ЗАНЯТТЯХ ІЗ ВИЩОЇ МАТЕМАТИКИ (НА ПРИКЛАДІ ПОЄДНАННЯ НА ПРАКТИЧНОМУ ЗАНЯТТІ З МАТЕМАТИЧНОЇ ФІЗИКИ ДВОХ ТЕМ: «РОЗВ'ЯЗУВАННЯ КРАЙОВИХ ЗАДАЧ ДЛЯ РІВНЯНЬ ЕЛІПТИЧНОГО ТИПУ, РОЗВ'ЯЗКАМИ ЯКИХ Є ПОЛІНОМИ ЛЕЖАНДРА», «ІСТОРІЯ ЖИТТЯ ТА НАУКИ АДРІЄН МАРІ ЛЕЖАНДРА»)

Цуканова А.О. 983
ЯК ЗАЦІКАВИТИ ПЕРШОКУРСНИКІВ ВИЩОЮ МАТЕМАТИКОЮ (НА ПРИКЛАДІ ЗАНЯТТЯ З ТЕМИ «СУМА ЧИСЛОВИХ РЯДІВ»)

Черньонков Я.О. 997
КОМУНІКАЦІЯ МАЙБУТНІХ БАКАЛАВРІВ ФІЛОЛОГІЇ В ПРОЦЕСІ МІЖКУЛЬТУРНІЙ ВЗАЄМОДІЇ

Широкова В.А. 1005
ФОРМУВАННЯ КОМУНІКАТИВНОЇ КОМПЕТЕНТНОСТІ МОЛОДШИХ ШКОЛЯРІВ ЗАСОБОМ «STORYTELLING»

Шмарко Н.С. 1015
МІЖНАРОДНИЙ ДОСВІД ВИХОВАННЯ ЕСТЕТИЧНОЇ КУЛЬТУРИ СТУДЕНТІВ ЗАКЛАДІВ ФАХОВОЇ ПЕРЕДВИЩОЇ ОСВІТИ

Юрченко О.В. 1027
СУБ'ЄКТНІСТЬ ЯК ПРОВІДНИЙ ЧИННИК ФОРМУВАННЯ ЦІЛІСНОСТІ ОСВІТНЬОГО ПРОСТОРУ

Юрченко В.Р. 1039
ОСОБЛИВОСТІ ВИХОВАННЯ ДІТЕЙ НАЦІОНАЛЬНИХ МЕНШИН НА ПРАВОБЕРЕЖНІЙ УКРАЇНІ У ХІХ – НА ПОЧАТКУ ХХ СТОЛІТТЯ

СЕРІЯ «Техніка»

Havrysh B.M., Kustra N.O., Holubnyk T.S. 1052
FEATURES OF REPRODUCTION OF PHOTOGRAPHIC IMAGES BY RISOGRAM METHOD

Kravchuk Ya.Ya. 1065
CROWDSOURCED DATA AND AL INTEGRATION IN ONLINE PLATFORMS FOR VOLUNTEER COLLABORATION

Polyakovska N.O., Bautina M.V. 1076
ASSESSING GENDER BIAS IN LARGE LANGUAGE MODELS USING UKRAINIAN-LANGUAGE TEXT

Батаєв С.В., Заплатинський Н.Б., Дмитрієнко О.О. 1091
АРХІТЕКТУРНІ ПІДХОДИ ДО ПОБУДОВИ РОЗПОДІЛЕНИХ СИСТЕМ ДЛЯ ОБРОБКИ ВЕЛИКИХ ДАНИХ

Білак Ю.Ю., Повханич В.І., Келемен М., Онуфрей О.В. 1105
ПРОГРАМНА ТЕХНОЛОГІЯ ВИВЕДЕННЯ РІВНЯ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ У РІЗНИХ РЕЖИМАХ

Білевський П.С. 1117
ЗМЕНШЕННЯ ЕЛЕКТРОМАГНІТНИХ ЗАВАД ІМПУЛЬСНИХ ПЕРЕТВОРЮВАЧІВ НАПРУГИ

Бондаренко Ю.А. 1128
ДВОРІВНЕВИЙ РОЗГЛЯД ТА ВРАХУВАННЯ НЕВИЗНАЧЕНОСТІ КОНТЕЙНЕРОПОТОКІВ В СИСТЕМІ МОРСЬКИХ ПЕРЕВЕЗЕНЬ

Вернигора Д.В., Карімов І.К. 1137
ЧИСЕЛЬНИЙ АЛГОРИТМ МОДЕЛЮВАННЯ МІСЦЕВОГО НАГРІВУ ВЕЛИКОГАБАРИТНИХ ВИРОБІВ В ГАЗОВИХ ПЕЧАХ

Гірний М.О., Левус Є.В. 1150
ЗАСТОСУВАННЯ ВЕЛИКОЇ МОВНОЇ МОДЕЛІ ДЛЯ НАДАННЯ ПЕРСОНАЛІЗОВАНИХ РЕКОМЕНДАЦІЙ У НАВЧАЛЬНІЙ СИСТЕМІ

Грачов О.А. 1162
ШТУЧНИЙ ІНТЕЛЕКТ В СІЛЬСЬКОМУ ГОСПОДАРСТВІ

Дохняк Б.О., Хавалко В.М. 1174
СТРУКТУРА ТА КОМПОНЕНТИ СУЧАСНОЇ ІНТЕЛЕКТУАЛЬНОЇ ТРАНСПОРТНОЇ МЕРЕЖІ

Думин І.Б., Жахалов В.В. 1186
АНАЛІТИЧНИЙ ОГЛЯД НАУКОВИХ СТАТЕЙ, ПОВ'ЯЗАНИХ З ТЕХНОЛОГІЯМИ РОЗВИТКУ ТА ДОВГОТРИВАЛОЮ ПАМ'ЯТТЮ ШТУЧНИХ ІНТЕЛЕКТУАЛЬНИХ АГЕНТІВ

Єврейнова Н.А., Журавель В.В. 1196
ДОСЛІДЖЕННЯ ВИТРАТ НА ВИКОНАННЯ РОБІТ З ФОРМУВАННЯ СТРАХОВОГО ФОНДУ ДОКУМЕНТАЦІЇ, ЩО ВКЛЮЧАЮТЬСЯ ДО ЗВЕДЕНОГО КОШТОРИСНОГО РОЗРАХУНКУ ВАРТОСТІ ОБ'ЄКТА БУДІВНИЦТВА

Жеребець О.М. 1209
ПОКРАЩЕННЯ БАГАТОПРОМЕНЕВОЇ РОЗДІЛЬНОЇ ЗДАТНОСТІ В СИСТЕМАХ ГЕОЛОКАЦІЇ RFID ЗА ДОПОМОГОЮ ВЕЙВЛЕТ-ПЕРЕТВОРЕННЯ

Карпин Д.С., Карпин А.В., Столярчук І.Д., Гарбич-Мошора О.Р., Войтович Х.О., Зіник О.О. 1219
ОПТИМІЗАЦІЯ ПРОЦЕСУ ОЦІНЮВАННЯ ТА ЗВІТНОСТІ ЗА ДОПОМОГОЮ GOOGLE WORKSPACE FOR EDUCATION

Кілімченко Д.О., Кузнєцов М.О., Устенко С.А. 1231
ВІДСТЕЖЕННЯ ДЕКІЛЬКОХ ОБ'ЄКТІВ В ІНТЕЛЕКТУАЛЬНІЙ СИСТЕМІ ВІДЕОСПОСТЕРЕЖЕННЯ

Кондратьєв С.Б. 1245
ЛОКАЛЬНИЙ МЕТОД ПОБУДОВИ КАРТИ ГЛИБИН НА БАЗІ АДАПТИВНОЇ СХЕМИ ЗІСТАВЛЕННЯ ТА АФІННИХ ІНВАРІАНТНИХ ОЗНАК

Кондращенко О.В. 1259
МОДЕЛІ ТА ІНСТРУМЕНТИ ТЕРИТОРІАЛЬНОГО ПЛАНУВАННЯ ЯК ОСНОВА СТРАТЕГІЧНОГО РОЗВИТКУ РЕГІОНІВ

Кононихін О.С., Бінькowська А.Б., Кононихіна О.О., Бурда В.С. 1269
СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ВИБОРУ ВУЗЛІВ СЕНСОРНОЇ МЕРЕЖІ В УМОВАХ НЕЧІТКОЇ ІНФОРМАЦІЇ

Кравченко В.М., Руденський Р.А., Волошин С.М., Корольчук В.І., Волошина Т.В. 1281
ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ПРОЄКТІВ МАШИННОГО НАВЧАННЯ В АГРОПРОМИСЛОВОМУ КОМПЛЕКСІ: МЕТОДИ ТА ПІДХОДИ ДО ПІДГОТОВКИ ДАНИХ

Лебідь О.В., Кіпоренко С.С. 1294
ІНТЕГРАЦІЯ ФРАКТАЛЬНОГО АНАЛІЗУ ТА МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ ТА КІБЕРНЕТИЧНИХ АТАК

Кривонос О.М. 1314
ВИКОРИСТАННЯ ГЕНЕРАТИВНОГО АІ ДЛЯ СТВОРЕННЯ ПРОГРАМНОГО КОДУ

Ліщук К.І., Родіонов П.Ю., Ткаченко В.В. 1326
ПРАКТИЧНІ АСПЕКТИ СТВОРЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ВИБОРУ НАПРЯМУ ОСВІТНЬОЇ ДІЯЛЬНОСТІ

Марцишин Р.С., Міюшкович Ю.Г., Щудло В.О. 1337
ОСОБЛИВОСТІ РОЗРОБКИ МУЛЬТИМЕДІЙНОЇ ВЕБ-ПЛАТФОРМА ДЛЯ ЦИФРОВІЗАЦІЇ ПОТРЕБ МАЛИХ ГРОМАД

Мельникова Н.І., Хайнас О.Ю. 1345
АНАЛІТИЧНИЙ ОГЛЯД НАУКОВИХ СТАТЕЙ ПОВЯЗАНИХ З ПРОГНОЗУВАННЯМ В ЕЛЕКТРОННІЙ КОМЕРЦІЇ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Ніколюк П.К. 1355
ІНТЕЛЕКТУАЛЬНИЙ НАВІГАЦІЙНИЙ АЛГОРИТМ ОПТИМАЛЬНОГО ВИБОРУ МАРШРУТУ ТРАНСПОРТНОГО ЗАСОБУ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Онищенко О.А., Мельник О.М., Курдюк С.В., Дрозденко О.І., Гаврилюк Т.К., Бурлаченко Д.А. 1372
ЗАСТОСУВАННЯ МЕТОДІВ МАШИННОГО НАВЧАННЯ ДЛЯ ОПТИМІЗАЦІЇ МАРШРУТІВ І ЗАВДАНЬ НАДВОДНИХ АВТОНОМНИХ АПАРАТІВ

Павленко В.С. 1387
РОЗВИТОК ТА ЗАСТОСУВАННЯ РАДІОЧАСТОТНОЇ ІДЕНТИФІКАЦІЇ (RFID) У ПРОМИСЛОВОСТІ

Паньків В.І., Сторожук О.Л. 1395
ВПРОВАДЖЕННЯ РОЗПОДІЛЕНИХ ЗГОРТКОВИХ НЕЙРОННИХ МЕРЕЖ ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ У РЕАЛЬНОМУ ЧАСІ У ПОТОКАХ ВЕЛИКИХ ДАНИХ

Парфенюк Т.М. 1407
ВИЯВЛЕННЯ ПОВТОРЮВАНОЇ МІЖКЛАСТЕРНОЇ ПОВЕДІНКИ АГЕНТІВ: СИСТЕМА МОНІТОРИНГУ СКООРДИНОВАНОЇ ДЕЗІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ

Резанова В.Г., Чупринка Н.В. 1420
ЧИСЕЛЬНІ МЕТОДИ РОЗВ'ЯЗАННЯ ТРАНСЦЕНДЕНТНИХ РІВНЯНЬ: ДОСЛІДЖЕННЯ ТА ПРОГРАМУВАННЯ

Римар П.В., Денисюк В.О., Огороднік М.О. 1433
ІНФОРМАЦІЙНА СИСТЕМА ДЛЯ ПІДТРИМКИ ІНДЕКСУВАННЯ ТА ПОШУКУ ІНФОРМАЦІЇ

Рощенко О.М. 1445
ОСНОВНІ ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ У СИСТЕМАХ GPS-НАВІГАЦІЇ

Семенишина І.В., Яценко О.І., Говорченко С.М. 1453
ІНТЕРАКТИВНЕ НАВЧАННЯ ПРОГРАМУВАННЮ ЗА ДОПОМОГОЮ ОНЛАЙН-КОМПІЛЯТОРІВ: ПРАКТИЧНИЙ ПІДХІД ДЛЯ PYTHON, C++ І JAVA

Семенів М.Р., Шовгенюк Й.В. 1467
МЕТОДИКА АНАЛІЗУ ТА ПОРІВНЯННЯ КОЛІРНИХ ПРОФІЛІВ ДЛЯ ДРУКУ НА ГЛЯНЦЕВИХ ТА МАТОВИХ ПОКРИТТЯХ

Сокол О.О. 1477
ПІДВИЩЕННЯ ПРОДУКТИВНОСТІ ДОМЕННО-СПЕЦІФІКОВАНОЇ ВЕЛИКОМОВНОЇ МОДЕЛІ ЗА ДОПОМОГОЮ МАШИННОГО НАВЧАННЯ

Сурова Н.М. 1489
МЕТОДОЛОГІЧНІ АСПЕКТИ ПРОГНОЗУВАННЯ КРЕАТИВНОСТІ ТА ІННОВАЦІЙНОСТІ ТЕХНІЧНОГО МИСЛЕННЯ В КОНТЕКСТІ НАУКОВОГО ПІЗНАННЯ

Тимченко О.В., Максимів М.Р. 1497
ДОСЛІДЖЕННЯ МЕТОДІВ ЗБІЛЬШЕННЯ РОЗДІЛЬНОЇ ЗДАТНОСТІ ЗОБРАЖЕНЬ

Тищенко Д.О., Франчук Т.М., Нікульшин Р.В. 1509
ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК ІНСТРУМЕНТ ЗАХИСТУ ДАНИХ НА ДЕРЖАВНИХ ПІДПРИЄМСТВАХ

Тищенко Д.О., Франчук Т.М., Кукса О.О. 1522
ІННОВАЦІЙНІ МЕТОДИ ОЦІНЮВАННЯ ЗАГРОЗ У БЕЗДРОТОВИХ МЕРЕЖАХ

Тищенко Д.О., Шестак Я.І., Чорний М.В. 1535
КОМПЛЕКСНИЙ ПІДХІД ДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ОРГАНІВ МІСЦЕВОГО САМОВРЯДУВАННЯ

Томашко А.П. 1546
ПРОГНОЗУВАННЯ ПОПИТУ В ЛОГІСТИЧНИХ МЕРЕЖАХ ЗА ДОПОМОГОЮ НЕЙРОННИХ МЕРЕЖЕВИХ АЛГОРИТМІВ

Федорін І.В., Семчук О.О. 1556
ПРОГНОЗУВАННЯ ЯКОСТІ СНУ ЗА ДАНИМИ ДЕННОЇ АКТИВНОСТІ ТА ДІЄТИ З ВИКОРИСТАННЯМ МАШИННОГО НАВЧАННЯ

Фрідлянд М.М. 1573
ПСИХОЛОГІЧНІ АСПЕКТИ СУЧАСНОГО ДИЗАЙНУ БУДІВЕЛЬ: СПЕЦИФІКА ВПЛИВУ АРХІТЕКТУРНИХ ЕЛЕМЕНТІВ НА ЕМОЦІЙНИЙ СТАН МЕШКАНЦІВ

Шакуров Є.О., Сурма Ю.Ю., Мінько Н.П. 1587
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ: ІННОВАЦІЙНІ ІНСТРУМЕНТИ ДЛЯ ПОКРАЩЕННЯ НАВЧАЛЬНОГО ПРОЦЕСУ

Ямковой М.В. 1600
МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ВПЛИВУ РОЗШИРЕННЯ ТРАНСПОРТНОЇ МЕРЕЖІ НА ОПТИМІЗАЦІЮ ЕФЕКТИВНОСТІ ДОСТАВКИ «ОСТАННЬОГО КІЛОМЕТРА» В МІСЬКИХ ЛОГІСТИЧНИХ СИСТЕМАХ

Яремко С.Б., Хавалко В.М. 1613
ВИКОРИСТАННЯ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ ДЛЯ ГЕНЕРУВАННЯ ПЕРСОНАЛІЗОВАНИХ РЕКОМЕНДАЦІЙ

СЕРІЯ «Фізико-математичні науки»

Дудик М.В. 1624
МОДЕЛЬ ДИНАМІКИ ТІСНОЇ ПОДВІЙНОЇ ЗОРЯНОЇ СИСТЕМИ "ЧЕРВОНИЙ ГІГАНТ – БІЛИЙ КАРЛИК"

№ 12(40) 2024
НАУКА і ТЕХНІКА СЬОГОДНІ
серії: право, економіка, педагогіка, техніка, фізико-математичні науки

УДК 004.67

https://doi.org/10.52058/2786-6025-2024-12(40)-1294-1313

Лебідь Олександр Васильович асистент кафедри комп'ютерних наук та цифрової економіки, Вінницький національний аграрний університет, м. Вінниця, тел.: (098) 888-26-06, https://orcid.org/0000-0003-4253-8696

Кіпоренко Світлана Сергіївна асистент кафедри комп'ютерних наук та цифрової економіки, Вінницький національний аграрний університет, м. Вінниця, тел.: (097) 034-30-45, https://orcid.org/0000-0001-5045-5052

ІНТЕГРАЦІЯ ФРАКТАЛЬНОГО АНАЛІЗУ ТА МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ ТА КІБЕРНЕТИЧНИХ АТАК

Анотація. У цій науковій статті розглядається важливе питання кібербезпеки - виявлення аномалій та кібернетичних атак у комп'ютерних системах. Для досягнення цієї мети автори пропонують інтегрувати два потужні методи - фрактальний аналіз та машинне навчання. Фрактальний аналіз використовується для аналізу та опису структурних властивостей даних, особливо у контексті часових рядів та сигналів. Він дозволяє виявляти складні, нелінійні залежності у даних, які можуть бути пов'язані з аномаліями в мережі або кібернетичними атаками. У даній статті ми пропонуємо метод інтеграції цих двох підходів для підвищення ефективності виявлення кібернетичних атак та аномалій у реальному часі. Представлено експериментальні результати, що демонструють високу точність та надійність запропонованого підходу.

Інтеграція фрактального аналізу та машинного навчання пропонує перспективний напрямок для посилення зусиль у галузі кібербезпеки. Поєднання цих двох методологій дозволяє дослідникам та практикам створювати більш надійний захист від кіберзагроз та своєчасно виявляти аномалії в комп'ютерних системах, що, зрештою, сприяє більш безпечному цифровому середовищу. Даний інтегрований підхід не лише підвищує точність виявлення аномалій, а й демонструє здатність адаптуватися до різноманітних мережевих середовищ і нових кіберзагроз. Оскільки цифрове середовище постійно розвивається, синергія фрактального аналізу та машинного навчання надає гнучке та ефективне рішення для захисту комп'ютерних систем. Дослідники та фахівці з кібербезпеки можуть використовувати цей метод, щоб випереджати кіберзловмисників та забезпечувати стійкість критичних мережевих інфраструктур. В умовах зростаючої важливості кібербезпеки це дослідження відкриває можливості для впровадження інноваційних стратегій, що зміцнюють наші цифрові захисні механізми.

Наше дослідження спрямоване на інтеграцію фрактального аналізу та машинного навчання для підвищення ефективності виявлення кібератак і аномалій у реальному часі. Фрактальний аналіз може виявляти складні взаємозв'язки у даних, тоді як машинне навчання допомагає розпізнавати шаблони та аномалії. Ми розробили метод, що поєднує ці два підходи, щоб досягти більш точного та надійного виявлення кібератак і аномалій у реальному часі, що підтверджується нашими експериментальними результатами.

Ключові слова: фрактальний аналіз, машинне навчання, виявлення аномалій, кібератаки, часові ряди, алгоритми класифікації, мережева безпека.

Lebid Oleksandr Vasyliovych Assistant of the Department of Computer Sciences and and digital economy, Vinnytsia National Agrarian University, Vinnytsia, tel.: (098) 888-26-06, https://orcid.org/0000-0003-4253-8696

Kiporenko Svitlana Sergiyivna Assistant of the Department of Computer Sciences and and digital economy, Vinnytsia National Agrarian University, Vinnytsia, tel.: (097) 034-30-45, https://orcid.org/0000-0001-5045-5052

INTEGRATION OF FRACTAL ANALYSIS AND MACHINE LEARNING FOR ANOMALY AND CYBERATTACK DETECTION

Abstract. This scientific article addresses a crucial issue in cybersecurity: the detection of anomalies and cyberattacks in computer systems. To achieve this goal, the authors propose integrating two powerful methods — fractal analysis and machine learning.

Fractal analysis is used to examine and describe the structural properties of data, particularly in the context of time series and signals. It enables the detection of complex, nonlinear dependencies in data that may be associated with network anomalies or cyberattacks. Machine learning, including classification and clustering algorithms, is applied to recognize patterns and anomalies within large datasets. It enhances anomaly detection accuracy and reduces the rate of false positives.

In this article, the researchers propose a method to integrate these two approaches, aiming to improve the efficiency of real-time cyberattack and anomaly detection. Experimental results demonstrate the high accuracy and reliability of the proposed approach. This article could be valuable for researchers and cybersecurity professionals seeking to strengthen the protection of computer systems against cyber threats.

The integration of fractal analysis and machine learning offers a promising direction for enhancing cybersecurity efforts. Combining these methodologies allows researchers and practitioners to develop more robust defenses against cyber threats and promptly detect anomalies in computer systems, ultimately contributing

to a safer digital environment. This integrated approach not only improves anomaly detection accuracy but also demonstrates adaptability to diverse network environments and emerging cyber threats.

As the digital landscape continues to evolve, the synergy between fractal analysis and machine learning provides a flexible and effective solution for protecting computer systems. Researchers and cybersecurity experts can leverage this method to stay ahead of cybercriminals and ensure the resilience of critical network infrastructures.

With the growing importance of cybersecurity, this study paves the way for implementing innovative strategies that strengthen our digital defense mechanisms. The number of cyberattacks and information security threats is rising annually, raising significant concerns about the reliability of organizational and individual operations. Cyberattacks are becoming increasingly sophisticated, with attackers continuously improving methods to bypass information system defenses.

Effective real-time monitoring systems are essential for detecting anomalies and cyberattacks. Traditional anomaly detection methods often rely on statistical approaches, which are not always effective in identifying complex, nonlinear anomalies. Moreover, many of these methods suffer from limited accuracy due to high false-positive rates or missed anomalies, reducing their overall effectiveness.

Adapting to new threats is also challenging, as changes in attack methods require constant updates to detection techniques, and traditional approaches often struggle to adapt quickly.

Our research focuses on integrating fractal analysis and machine learning to enhance the real-time detection of cyberattacks and anomalies. Fractal analysis can uncover intricate relationships in data, while machine learning aids in pattern and anomaly recognition. We have developed a method that combines these two approaches to achieve more accurate and reliable real-time detection of cyberattacks and anomalies, as validated by our experimental results.

Keywords: fractal analysis, machine learning, anomaly detection, cyberattacks, time series, classification algorithms, network security.

Постановка проблеми. У сучасному цифровому світі, де обмін та обробка інформації досягли безпрецедентних масштабів, кібербезпека стала надзвичайно важливим питанням для організацій та окремих осіб. Кібератаки становлять загрозу, яка може призвести до значних наслідків, включаючи порушення конфіденційності даних, збої в доступності послуг та значні фінансові втрати.

Теорія фракталів і мультифракталів нині широко використовується для опису властивостей самоподібності та складного масштабування, які спостерігаються у багатьох застосуваннях. Множина фракталів включає об'єкти (лінії, поверхні, тіла), які мають дуже рельєфну форму і демонструють певну

повторюваність на широкому діапазоні масштабів [1]. Однак не лише геометричні форми об'єктів мають фрактальну структуру; часові характеристики процесів і явищ, що відбуваються у середовищах з самоподібною структурою, також проявляють фрактальну поведінку. Фрактальні часові ряди є цілим класом фрактальних кривих, які широко використовуються для опису та моделювання різноманітних явищ.

Часовий ряд являє собою послідовність значень досліджуваної величини, записаних з регулярними інтервалами. Як правило, випадкові зміни величин представлені у вигляді рядів, найпопулярнішими прикладами яких є коливання валютних курсів та тимчасові зміни інших економічних показників. Природне представлення спостережень природних явищ також зводиться до часових рядів вимірювань температури повітря, опадів, швидкості вітру та інших метеорологічних даних. Часові ряди широко використовуються в медицині, найяскравішим прикладом чого є електрокардіограма серця, а також у описі стохастичних процесів у фізиці, хімії, соціології та інших науках і технологіях.

Для виявлення кібератак та аномалій у комп'ютерних системах дослідники та практики розробляють інноваційні методи та технології. У цьому контексті два основні підходи виділяються: фрактальний аналіз та машинне навчання. Фрактальний аналіз є потужним інструментом для аналізу складних структур даних і взаємозв'язків. Його застосування в кібербезпеці дозволяє ідентифікувати нелінійні та складні залежності в часових рядах і сигналах, які можуть вказувати на аномальні дії в мережах.

Машинне навчання, з іншого боку, надає можливість автоматизувати виявлення аномалій, навчаючи моделі розпізнавати відхилення від регулярних шаблонів на основі історичних даних. Це допомагає підвищити точність виявлення аномалій та знизити кількість хибнопозитивних результатів.

Однак кожен із цих методів, застосований окремо, має свої обмеження та недоліки. У цій статті ми досліджуємо можливість інтеграції фрактального аналізу та машинного навчання для створення ефективної системи виявлення кібератак і аномалій, яка використовує сильні сторони обох підходів.

Аналіз останніх досліджень та публікацій. Аналіз останніх досліджень і публікацій щодо інтеграції фрактального аналізу та машинного навчання в контексті виявлення аномалій і кібератак підтверджує активний інтерес наукової спільноти та практиків у цій галузі.

Перш за все, багато досліджень зосереджуються на вдосконаленні алгоритмів фрактального аналізу для аналізу мережевого трафіку та даних безпеки. Це включає розробку нових методів для виділення фрактальних ознак, які можуть бути цінними для виявлення аномалій. Деякі з цих робіт досліджують застосування фрактального аналізу для виявлення нелінійних залежностей у часових рядах мережевої активності [10].

З іншого боку, численні дослідження підкреслюють розвиток алгоритмів машинного навчання для виявлення аномалій у кіберсфері. Застосування глибокого навчання, нейронних мереж та інших методів машинного навчання стає все більш поширеним. Іншим важливим напрямом є розробка ансамблевих моделей, які поєднують різні підходи для підвищення точності виявлення аномалій [6].

Публікації також акцентують увагу на важливості інтеграції цих двох підходів. Деякі статті пропонують гібридні системи, що поєднують фрактальний аналіз і машинне навчання для підвищення ефективності виявлення аномалій та кібератак. Ці підходи можуть включати використання фрактальних ознак для попередньої обробки даних перед подачею їх у моделі машинного навчання [9].

Загалом, сучасні дослідження свідчать про розробку інтегрованих методів, які поєднують найкращі практики фрактального аналізу та машинного навчання для вдосконалення систем виявлення кібератак та аномалій у реальному часі.

Метою дослідження є розробка та впровадження ефективної системи для виявлення аномалій та кібератак у комп'ютерних мережах на основі інтеграції методів фрактального аналізу та машинного навчання.

Виклад основного матеріалу. Вплив комп’ютерних атак (СА) посилюється частим використанням застарілих операційних систем, неефективними механізмами безпеки та численними вразливими місцями в незахищених мережевих протоколах. Ці вразливості дозволяють зловмисникам маніпулювати налаштуваннями мережевих пристроїв, перехоплювати та перенаправляти трафік, порушувати мережевий зв’язок і отримувати несанкціонований доступ до внутрішніх компонентів системи. Отже, такі ЦС призводять до аномальної активності в мережевому трафіку

Для постійного моніторингу мережевого трафіку, виявлення аномалій, ідентифікації та класифікації атак і виявлення несанкціонованих змін важливо проаналізувати великий набір параметрів, які характеризують нові властивості трафіку. Водночас важливо підтримувати високу якість обслуговування заявок. Ця проблема спонукає до пошуку інноваційних методів виявлення СА та захисту передачі даних. Методологія, запропонована в цій статті - інтеграція фрактального аналізу з машинним навчанням - являє собою один із таких підходів. Фрактальний аналіз дозволяє швидко виявляти аномальний трафік, тоді як методи машинного навчання допомагають ідентифікувати, класифікувати та прогнозувати ЦС.

Показник Херста, також відомий як показник масштабування, є центральним параметром у фрактальному аналізі. Він в основному використовується в аналізі часових рядів, де нижчі значення експоненти Херста вказують на триваліші часові затримки між ідентичними парами значень у

часовому ряді. Визначення того, стаціонарний процес чи ні, допомагає вибрати алгоритм для обчислення цього показника, який відіграє вирішальну роль у виявленні аномалій.

Дослідження показали, що штучні нейронні мережі, зокрема мережі LSTM (довгокороткочасної пам'яті), є високоефективними для ідентифікації, класифікації та прогнозування КА [16]. Мережі LSTM, підтип рекурентних нейронних мереж, можуть зберігати та використовувати інформацію з попередніх часових кроків, дозволяючи їм ефективно аналізувати послідовності даних. Ця характеристика робить їх особливо придатними для моделювання динаміки подій у часі, позиціонуючи їх як цінні інструменти кібербезпеки.

Використання мереж LSTM дозволяє виявляти складні залежності та шаблони в мережевому трафіку, які часто складно або навіть неможливо виявити за допомогою звичайних методів статистичного або фрактального аналізу. Навчаючись на історичних даних, мережі LSTM можуть ідентифікувати та класифікувати нові аномалії як певні типи СА [10]. Крім того, вони володіють можливостями прогнозування, що дозволяє передбачати потенційні кібератаки на основі виявлених аномалій і визначених залежностей. Цей функціонал дозволяє своєчасно реагувати та впроваджувати захисні заходи.

Для ефективного виявлення та класифікації ЦС методологія починається з визначення того, чи є мережевий трафік стаціонарним чи нестаціонарним. Після цього розраховується експонента Херста, що дозволяє виявити самоподібність у трафіку. Варіації показника Херста сигналізують про аномалії в мережевому трафіку, часто вказуючи на активність ЦС. На наступних етапах проводиться ідентифікація та класифікація СА з подальшою розробкою заходів захисту системи передачі даних з використанням мереж LSTM [8-10].

Сучасні системи моніторингу все частіше використовують аналіз самоподібності в даних часових рядів як метод виявлення аномалій. Самоподібність означає, що структура системи залишається незмінною навіть при спостереженні в різних масштабах — характеристика, яка спостерігається як у природних, так і в штучних системах, включаючи мережевий трафік. Для виявлення самоподібності використовується кілька підходів, зокрема:

- R/S Analysis Method. Цей метод порівнює діапазон часового ряду в різних масштабах і вважається одним із найпростіших методів оцінки самоподібності.
- Показник Херста. Даний параметр є центральним для визначення самоподібності в часовому ряду.
- Фрактальна розмірність. Міра, яка характеризує складність часового ряду, часто використовується в поєднанні з іншими методами.

Вивчення самоподібності в системах моніторингу дає кілька переваг:

- Покращене виявлення аномалій. Шляхом розпізнавання складних шаблонів, незмінних за масштабом, цей підхід може виявити аномалії, які традиційні методи можуть пропустити.

- Оцінка стану системи та прогнозування. Аналіз самоподібності може допомогти контролювати стан системи та передбачити потенційні проблеми, спостерігаючи повторювані моделі в різних масштабах.

Незважаючи на потенціал цих методів, практичні експерименти, зосереджені на фрактальних властивостях мережевого трафіку, обмежені.

Машинне навчання є потужним інструментом для виявлення мережевих атак із кількома помітними перевагами:

1. Здатність навчатися на великих обсягах даних - моделі машинного навчання чудово аналізують великі набори даних, дозволяючи виявляти ширший діапазон атак, ніж статистичні методи.
2. Адаптованість до нових типів атак - у міру розвитку мережевих атак моделі машинного навчання можуть постійно навчатися на свіжих даних, покращуючи реакцію на нові загрози.
3. Виявлення комплексних прихованих атак - машинне навчання може ідентифікувати складні приховані атаки, наприклад ті, що використовують приховані канали даних.

Незважаючи на ці сильні сторони, машинне навчання має обмеження, зокрема складність конфігурації моделі та потенційну потребу у великих навчальних даних. Крім того, у деяких випадках статистичні методи аналізу можуть досягти більшої точності.

Загалом інтеграція аналізу самоподібності, вимірювання ентропії та машинного навчання забезпечує багатогранний підхід до кібербезпеки, особливо в корпоративних мережах, де захист від дедалі складніших кібератак є надзвичайно важливим. Поєднання цих методів пропонує динамічну та адаптовану структуру для моніторингу, виявлення та ефективного пом'якшення загроз безпеці.

Результати. Інтеграція фрактального аналізу та машинного навчання знаменує значний прогрес у виявленні аномалій та кібербезпеці. Фрактальний аналіз ефективно виявляє самоподібні моделі в мережевому трафіку, дозволяючи раннє виявлення відхилень від нормальної поведінки трафіку. Машинне навчання, зокрема через мережі довготривалої короткочасної пам'яті (LSTM), покращує ідентифікацію складних моделей, пов'язаних з аномаліями, забезпечуючи як точність, так і надійність у виявленні як відомих, так і невідомих загроз. Разом ці методи підтримують точну та надійну ідентифікацію аномалій.

Обробка в режимі реального або майже в реальному часі є основною особливістю цієї комбінованої методології, яка має вирішальне значення для зменшення впливу кібератак шляхом сприяння швидкому реагуванню. Експериментальні оцінки демонструють високу ефективність, що робить запропонований підхід ідеальним для реалізації в сучасних мережах передачі даних. Використовуючи сильні сторони як фрактального аналізу, так і

машинного навчання, ця методологія пропонує потужне рішення для підвищення безпеки мережі.

У даному дослідженні мережевий трафік моделюється як часовий ряд X={x1,x2,…,xп}X={ x_1,x_2,…,x_n}, що описується через фрактальний броунівський рух (FBM). Випадковий процесX(t)X (t)пов'язаний з FBM характеризується параметром ХерстаXX, де0≤X≤10≤X≤1. Прирости цього процесуΔX(τ)=X(t+τ)−X(t)Δ X (τ)=X (m+τ)−X (t)слідувати нормальному розподілу, забезпечуючи статистичну основу для виявлення аномалій у даних часових рядів. Ця модель полегшує виявлення змін у поведінці трафіку, які можуть означати кібератаки, таким чином формуючи основу для стратегій захисту мережі в режимі реального часу.

$$P(\Delta X(\tau) < x) = \frac{1}{\sqrt{2\pi\delta\tau^{2H}}} \int_{-\infty}^{x} exp\left[-\frac{z^2}{2\delta_0^2\tau^{2H}}\right] dz, \qquad (1)$$

- де, $P(\Delta X(\tau)<x)$ - це ймовірність того, що приріст FBM $\Delta X(\tau)$ процесу буде меншим за задане значення x.
- $\frac{1}{\sqrt{2\pi\delta\tau^{2H}}}$ - є нормувальною константою, що забезпечує ймовірність усіх можливих значень $\Delta X(\tau)$ дорівнює 1.
- $\int_{-\infty}^{x} exp\left[-\frac{z^2}{2\delta_0^2\tau^{2H}}\right] dz$ - інтеграл, що обчислює ймовірність того, що приріст процесу FBM $\Delta X(\tau)$ буде меншим за значення x.
- z - змінна інтегрування.

Формула заснована на припущенні, що приріст процесу FBM ΔX(τ) відповідає нормальному розподілу із середнім значенням 0 і дисперсією $2\delta_0^2\tau^{2H}$. Це означає, що ймовірність того, що приріст процесу FBM ΔX(τ) буде меншим за задане значення x, можна розрахувати за допомогою нормального розподілу. Формула (1) використовується для виявлення аномалій у мережевому трафіку. Якщо ймовірність того, що приріст процесу FBM ΔX(τ) буде меншим за задане значення x, низька, це може бути ознакою аномалії. Наприклад, якщо ми встановимо значення x рівним 3 стандартним відхиленням, то ймовірність того, що приріст процесу FBM ΔX(τ) буде меншим за x, буде дуже низькою (приблизно 0,00135%). Це означає, що якщо приріст процесу FBM ΔX(τ) перевищує 3 стандартні відхилення, це вважається аномалією.

Параметр Херста H характеризує ступінь самоподібності процесу. Чим ближче цей параметр до 1, тим більше виражені фрактальні властивості. H = 0,5 свідчить про відсутність самоподібності. FBM з H = 0,5 збігається до класичного броунівського руху, роблячи часовий ряд найбільш шумним. Виявлення аномалій у мережевому трафіку за допомогою фрактального

аналізу виконується наступним чином. Спочатку визначається, чи є рух нерухомим. Для цього використовується тест Дікі-Фуллера. Потім одним із методів розраховується значення H залежно від того, є рух нерухомим чи ні. Якщо рух нерухомий, використовується метод R/S. Якщо рух нестаціонарний, використовується метод DFA. Якщо значення H потрапляє в діапазон [0,5; 1], то трафік вважається нормальним, тобто аномалій немає. В іншому випадку трафік вважається аномальним, що вказує на наявність аномалій.

Наступним кроком у нашому дослідженні було створення коду Python, який поєднує фрактальний аналіз і машинне навчання для виявлення аномалій і кібератак (рис. 1).

```
import numpy as np
import matplotlib.pyplot as plt

# R/S method to calculate Hurst exponent
def hurst_exponent(time_series):
    N = len(time_series)
    T = np.cumsum(time_series - np.mean(time_series))  # Cumulative sum
    R = np.max(T) - np.min(T)  # Range
    S = np.std(time_series)  # Standard deviation
    return np.log(R/S) / np.log(N)
# Example network traffic data (replace with your actual data)
network_traffic = np.random.normal(0, 1, 1000)  # Simulating network traffic as random data

# Calculate Hurst exponent
H = hurst_exponent(network_traffic)
print(f»Hurst Exponent (H): {H}»)
```

Рис. 1 Фрактальний аналіз (метод R/S)

Джерело: власна розробка авторів

Метод R/S допомагає оцінити параметр Херста (H) для заданого часового ряду.

Після виконання фрактального аналізу ми можемо використовувати модель LSTM для виявлення аномалій у даних часових рядів (мережевий трафік). Моделі LSTM підходять для завдань передбачення послідовності, і ми навчимо модель передбачати наступні часові кроки в серії. Якщо прогноз моделі значно відхиляється від фактичних даних, це може бути аномалією (рис. 2).

```
import pandas as pd
import numpy as np
```

```
from sklearn.preprocessing import MinMaxScaler
from tensorflow.keras.models import Sequential
from tensorflow.keras.layers import LSTM, Dense

# Prepare time series data for LSTM model
def prepare_data(data, n_steps):
    X, y = [], []
    for i in range(len(data)):
        end_ix = i + n_steps
        if end_ix > len(data)-1:
            break
```

Рис. 2 Виявлення аномалій за допомогою LSTM (довгокороткочасної пам’яті)

Джерело: власна розробка авторів

Окрім методів фрактального аналізу, існує багато інших технік для виявлення аномалій у часових рядах. До цих методів належать авторегресивна інтегрована ковзаюча середня (ARIMA), кумулятивні суми, метод опорних векторів (SVM), випадковий ліс (RF) та інші. Ці методи відзначаються ефективністю у виявленні аномальних сплесків. У випадку таких сплесків аномалії виявляються як нестійкість у деяких спостережуваних часових рядах. Ці аномалії проявляються не лише у вигляді раптових стрибків амплітуд вимірювань, а й у вигляді повільних тенденцій, які практично непомітні за період спостереження.

Однак під час тестування зазначених алгоритмів на реальних даних мережевого трафіку було виявлено, що не всі аномальні значення в трафіку є обов'язково аномаліями. Тому запропонована методологія передбачає додаткове використання машинного навчання для виявлення аномалій, заснованого на гібридній штучній нейронній мережі, яка складається з автоенкодера та класифікатора.

Структура гібридної нейронної мережі, розробленої для виявлення незвичних явищ у стаціонарній мережі, представлена на рис. 3

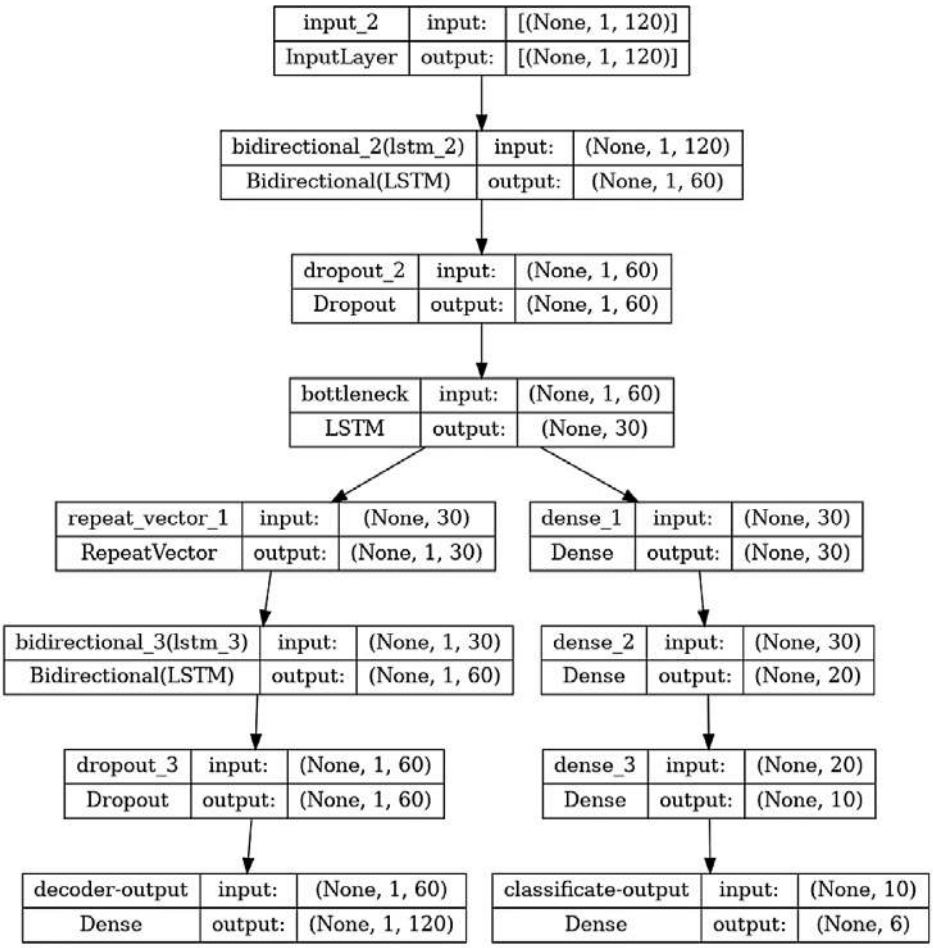


Рис. 3 Модель гібридної нейронної мережі

Джерело: власна розробка авторів

Гібридна мережа складається з різних шарів, кожен з яких виконує свою специфічну задачу. Основні шари включають: • Шар «Dropout» - призначений для вирішення проблеми перенавчання в нейронних мережах. • Шар «Bidirectional» - дозволяє здійснювати глибоке генеративне навчання, при якому вихідний шар може одночасно отримувати інформацію з минулих (зворотних) і майбутніх (прямих) станів. • Шар «Bottleneck» - зменшує кількість ознак і, відповідно, кількість операцій в кожному шарі, що забезпечує швидкість результатів.

Вхідний шар гібридної нейронної мережі містить 120 нейронів, які використовуються як для автокодувальника, так і для класифікатора.

Для автокодувальника використовуються шари типу LSTM. LSTM мережі є підтипом більш загальних рекурентних нейронних мереж. Однією з їхніх ключових особливостей є здатність зберігати інформацію (стан клітини) для майбутнього використання. LSTM може видаляти інформацію з стану клітини, і цей процес контролюється фільтрами. Фільтри дозволяють інформації проходити через мережу за певними умовами. Фільтри складаються з

шару сигмоїдної нейронної мережі та операцій елементного множення. Шар сигмоїди повертає значення від нуля до одного, визначаючи, яку частину інформації слід пропускати через мережу. Нуль у цьому випадку означає «не пропускати нічого», а одиниця - «пропускати все».

Рекурентність дозволяє штучній нейронній мережі «посилатися» на свої минулі результати, аналізуючи прогнози. Таким чином, контекст майбутніх рішень залежить не тільки від початкового глибокого навчання LSTM, а й від її постійної роботи в потоці.

Під час навчання гібридної нейронної мережі вхідний шар отримує різні вектори, які представляють інформацію, зібрану з даних. Ці вектори можуть містити різні ознаки, важливі для аналізу даних і класифікації.

Нейронна мережа обробляє ці вектори, використовуючи свої внутрішні ваги та параметри. Після обробки вхідних векторів мережа намагається знайти шаблони в даних і зробити спробу класифікації їх у конкретні категорії або класи. Важливим аспектом навчання є оптимізація параметрів мережі, щоб вона ефективно виконувала завдання, що стоять перед нею, включаючи виявлення аномалій або аналіз даних. Тривалість та результати навчання залежать від різних факторів, зокрема обсягу даних, архітектури мережі та методів оптимізації.

На рис. 4 можна наочно спостерігати процес навчання гібридної нейронної мережі за допомогою різних векторів (підпослідовностей, послідовностей або вбудовувань).

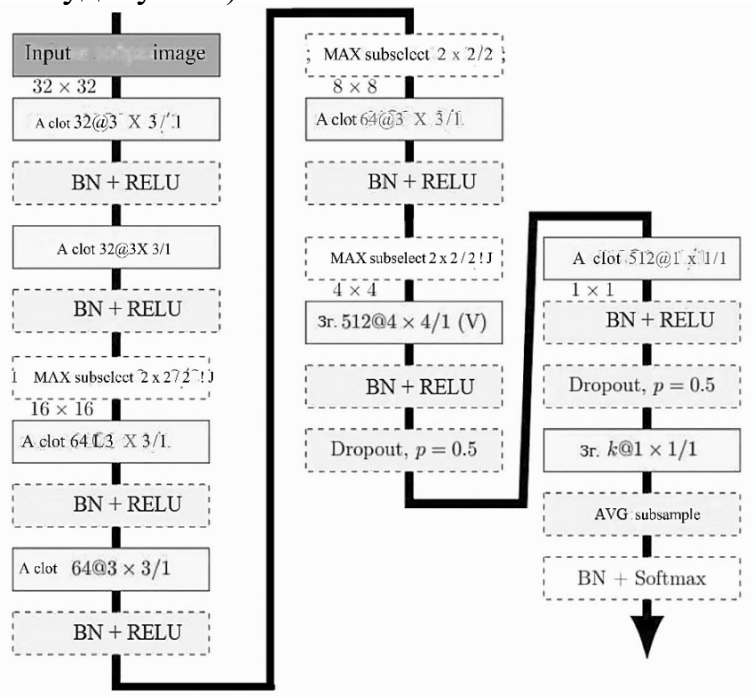


Рис. 4 Графічна інтерпретація векторного представлення даних, що надходять на вхід гібридної нейронної мережі

Джерело: власна розробка авторів

Даний малюнок ілюструє кібердіапазон, розроблений для тестування методології на реальних даних для оцінки її точності та ефективності. Він включає кілька пристроїв, які зазвичай використовуються для кібератак, наприклад Kali Linux (операційна система кібербезпеки, яка використовується для тестування на проникнення), Metasploitable (віртуальна машина, створена для симуляції атак) і Damn Vulnerable Web Application (навмисно вразлива веб-програма). Показані мережеві пристрої включають брандмауер, маршрутизатор і комутатор, які можна використати під час кібератак. Уразливі системи, такі як Windows 10 і Ubuntu Server, також зображені, підкреслюючи цілі потенційних порушень безпеки. Це налаштування забезпечує контрольоване середовище для тестування методології виявлення аномалій і ідентифікації кібератак (рис.5).

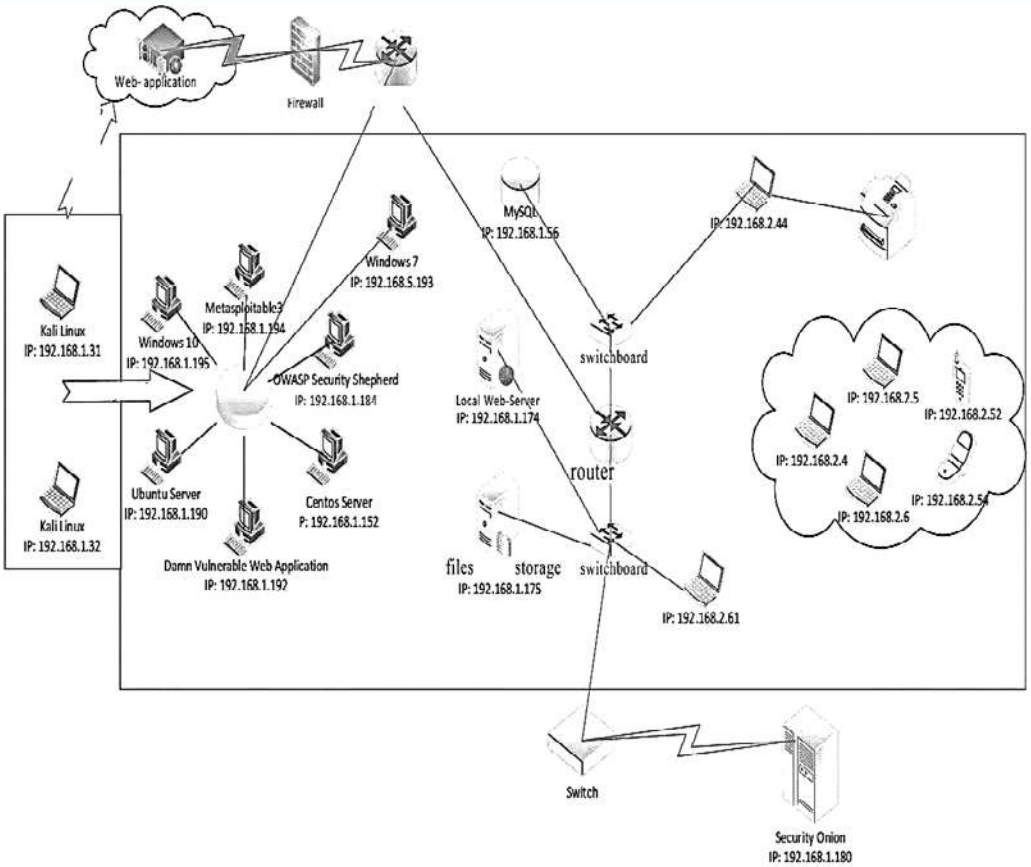


Рис. 5 Кібердіапазон для експериментальної оцінки методології виявлення аномалій і кібератак у розподілених системах

Джерело: побудовано авторами на основі проведених досліджень

У рамках тестування методів виявлення аномалій в кібердіапазоні було проведено 30 видів кібератак та зібрано 40 ГБ легітимного мережевого трафіку. Трафік був записаний у pcap-файли та використаний для створення датасету за допомогою інструментів Netsniff-ng і Bro. Для виявлення аномалій

застосовувались методи кумулятивної суми, Random Forest (RF) та Support Vector Machines (SVM). Було виявлено, що не кожне збільшення активності є аномалією, оскільки мережевий трафік може мати самоподібність, що ускладнює виявлення зловмисної активності на основі лише обсягу трафіку. Тестування проводилось на емітованій мережі в GNS3, де були враховані параметри мережевого обладнання та протоколи (табл.1).

Таблиця 1.

Атрибути згенерованого датасету

Атрибут	Тип	Опис
Flow.ID	Числовий	Ідентифікатор потоку
Source.IP	Рядок	IP-адреса джерела
Destination.IP	Рядок	IP-адреса призначення
Source.Port	Числовий	Порт джерела
Destination.Port	Числовий	Порт призначення
Protocol	Рядок	Протокол
Packet.Number	Числовий	Кількість пакетів
Packet.Length.Mean	Числовий	Середня довжина пакету
Packet.Length.Min	Числовий	Мінімальна довжина пакету
Packet.Length.Max	Числовий	Максимальна довжина пакету
Packet.Length.Variance	Числовий	Дисперсія довжини пакету
Packet.Length.Skewness	Числовий	Скошеність довжини пакету
Packet.Length.Kurtosis	Числовий	Куртозис довжини пакету
Time.First.Packet	Числовий	Час першого пакету
Time.Last.Packet	Числовий	Час останнього пакету

Джерело: узагальнено авторами на основі проведених досліджень

Таблиця містить 14 атрибутів, що використовуються для виявлення кібернападів. Ці атрибути описують різні аспекти мережевого трафіку, такі як ідентифікатор потоку, IP-адреси джерела та призначення, порти, протокол, кількість пакетів, довжина пакетів та час першого та останнього пакету. Атрибути, як-от Packet.Number, Packet.Length.Mean і Packet.Length.Variance, використовувалися для виявлення аномалій у мережевому трафіку. Наприклад, якщо кількість пакетів у потоці значно перевищувала середнє значення, це вважалося індикатором кібернападу. Інші атрибути, такі як Source.IP, Destination.IP та Protocol, використовувалися для виявлення кібернападів, які включали специфічні IP-адреси, порти та протоколи.

Для оцінки точності та повноти виявлення аномалій на навченій нейронній мережі спочатку був використаний датасет з кібернападами для навчання. Результати показали, що точність виявлення аномалій у цьому випадку склала 96,9%.

Рис. 6 ілюструє динаміку точності та функції втрат класифікатора протягом 300 циклів навчання (епох). Цей графік показує, як модель покращувала свою адаптацію до навчальних даних з часом і збільшувала точність виявлення

аномалій. На основі результатів цього аналізу можна зробити висновок, що навчена нейронна мережа продемонструвала високу точність у виявленні аномалій після навчання на датасеті з кібернападами.

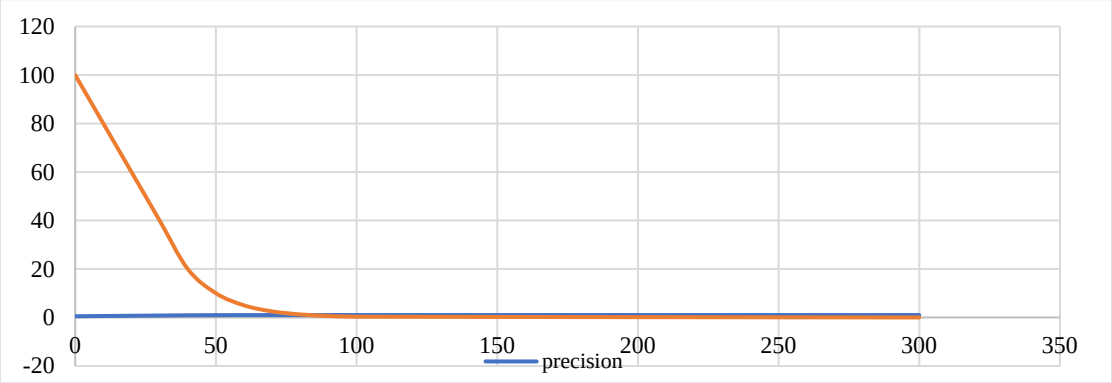


Рис. 6 Точність та функція втрат нейронної мережі

Джерело: побудовано авторами на основі проведених досліджень

На графіку показано, що з просуванням епох навчання покращуються як точність, так і функція втрат. Спочатку точність класифікатора становить 50%, тобто мережа може правильно класифікувати лише половину аномалій. Проте з кожною епохою навчання точність поступово зростає і досягає 96,9% на 300-й епосі. Це демонструє здатність мережі правильно класифікувати 96,9% аномалій. Крім того, функція втрат з часом зменшується, що вказує на ефективне навчання мережі. У 300-й епосі функція втрат дуже низька і становить 0,0004, що підтверджує, що мережа добре навчена.

Поряд з експериментом з виявлення аномалій також проводився експеримент з класифікації кібератак. Для оцінки продуктивності класифікатора та вибору відповідного порогу розрізнення для поділу на класи використовувалися крива ROC (операційна характеристика приймача) і крива PR (точність запам’ятовування), як показано на рис.7.

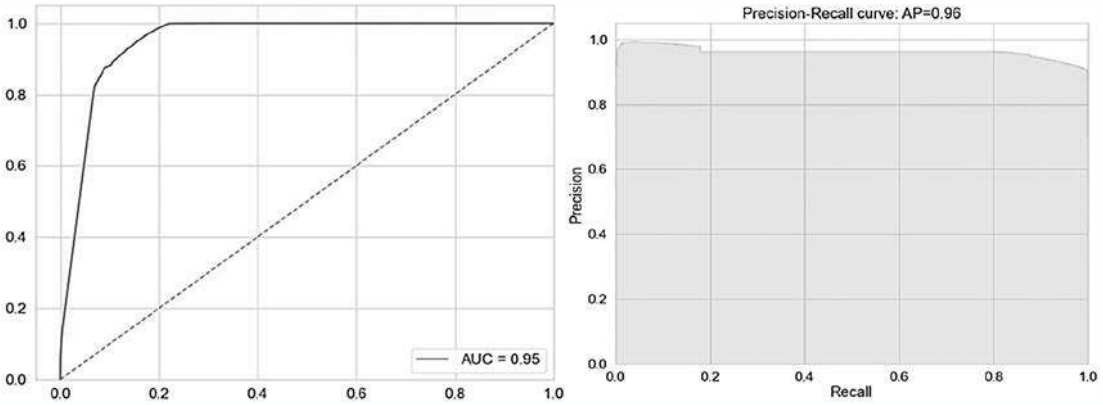


Рис. 7 Крива ROC і крива Precision-Recall для моделі на основі 5 ознак

Джерело: побудовано авторами на основі проведених досліджень

Під час класифікації аналізованого мережевого трафіку за допомогою розроблених моделей були розраховані числові значення для кривих ROC і Precision-Recall (PR). З них було отримано значення площі під кривою (AUC) для обох кривих. Значення AUC відображають ефективність класифікатора з оцінкою 0,95 для кривої ROC і 0,96 для кривої PR,

Наступний етап дослідження включав розрахунок градієнта помилок аналізованого трафіку. У нейронних мережах градієнт помилок допомагає визначити, як зміни конкретного параметра впливають на функцію помилок.

Похибка визначається як різниця між фактичним значенням і прогнозованим значенням. Градієнт помилки — це вектор, який вказує в напрямку, де помилка зменшується найшвидше. Похибку можна обчислити за допомогою sin

$$E = (y - f(x))^2 \quad (2)$$

де: E - помилка y - фактичне значення f(x) - прогнозоване значення. Градієнт помилок визначається за такою формулою:

$$g = 2(0) * f(5)$$
$$g = 0 \quad (3)$$

де: g - градієнт помилки f'(x) - похідна функції f(x).

З графіка видно, що похибка має мінімум у точці ваги (рис.7). Це означає, що для цієї точки фактичне значення дорівнює прогнозованому значенню, тобто похибка дорівнює нулю. У ваговій точці 5 градієнт помилки дорівнює нулю. Це означає, що похибка не змінюється в цьому напрямку. Отже, ми зробили наступні розрахунки:

Помилка ваги 5

$$E = (5 - f(5))^2$$
$$E = 0$$

Градієнт помилок для ваги 5

$$g = 2(5 - f(5)) * f5$$
$$g = 2(0) * f(5)$$
$$g = 0$$

Отже, розрахунки підтверджують, що помилка мінімальна при значенні ваги 5, а градієнт помилки дорівнює нулю в цій точці. Метод використовує вектор градієнта для визначення напрямку, в якому функція помилки зменшується найшвидше. Це дозволяє «спускатися схилом помилки», наближаючись до мінімального значення функції. Параметри моделі оновлюються на кожній ітерації та рухаються в напрямку, протилежному градієнту функції помилки, поки не буде знайдено точку в просторі параметрів, де помилка на навчальних даних є мінімальною.

Візуальний аналіз підтвердив високу точність запропонованого підходу з мінімальною кількістю хибнопозитивних результатів. Для більш всебічної оцінки було визначено основні метрики класифікації атак (табл. 2), включаючи точність, повноту та F1-міру. F1-міра представляє гармонійне середнє між точністю та повнотою і слугує комплексним показником для оцінки ефективності класифікації атак.

Таблиця 2.

Ключові метрики класифікації атак

Клас Атаки	Точність	Повнота	F-міра
XXE	0,95	0,88	0,91
Ін'єкція шаблонів на стороні сервера	0,99	1	0,99
SQL-ін'єкція	0,96	0,95	0,95
Траверсал	0,94	0,86	0,9
Кодування траверсалу	0,99	0,99	0,99
Середнє	0,95	0,91	0,92

Джерело: узагальнено авторами на основі проведених досліджень

На основі даних у таблиці можна зробити висновок, що система класифікації атак має досить високу ефективність. Середні значення точності, повноти та F-міри для всіх класів атак перевищують 0,9. Це означає, що система правильно класифікує більшість атак і не пропускає багато з них.

У загальному, запропонована методологія є найбільш підходящою для завдань з високими вимогами до точності і швидкості виявлення, тоді як інші методи можуть бути кращими залежно від специфічних вимог до економічної ефективності та складності впровадження.

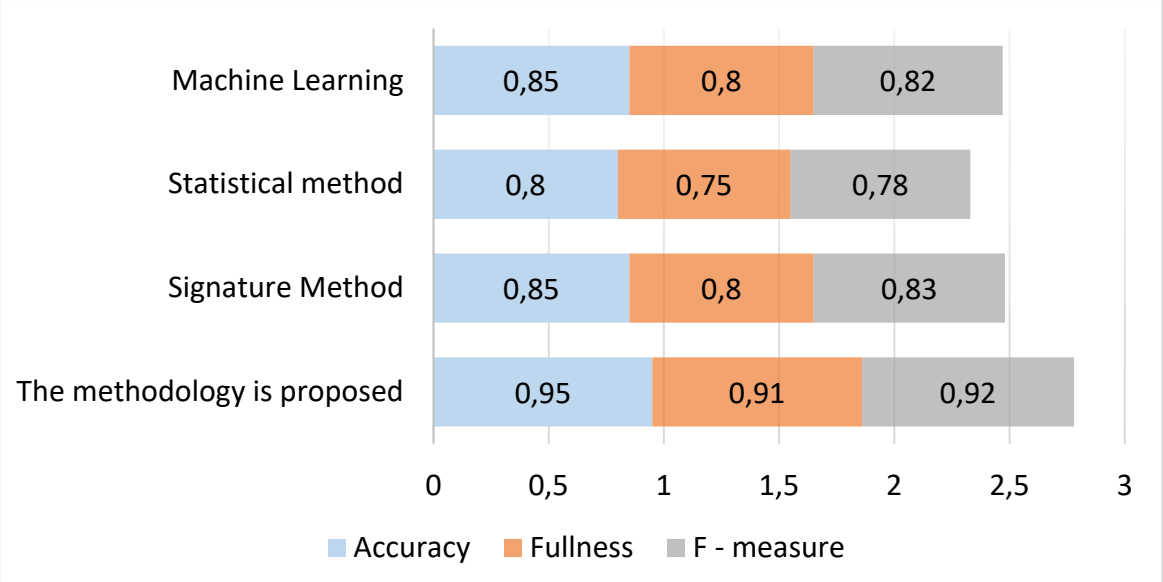


Рис. 8 Графічне зображення показників для оцінки виявлення відомих космічних апаратів

Джерело: побудовано авторами на основі проведених досліджень

Слід зазначити, що додатковою перевагою запропонованого методу є його здатність виявляти аномалії в трафіку будь-якого типу. Інші відомі методи добре працюють лише в умовах стаціонарного трафіку.

Серед інших переваг цього підходу слід відзначити його нечутливість до параметрів мережі, таких як пропускна здатність і протокол, а також здатність адаптуватися до різних умов трафіку. Це робить запропонований метод високо гнучким і підходящим для використання в різних мережевих середовищах. Крім того, цей метод вирізняється високою точністю і повнотою при виявленні аномалій, що робить його відмінним вибором для захисту мереж від кібернападів. Попри помірну складність впровадження, ця методологія має потенціал для вирішення багатьох задач кібербезпеки та може бути застосована в різних галузях, де виявлення аномалій у мережевому трафіку є критично важливим.

Крім того, запропонований підхід є універсальним завдяки представленню процесів у вигляді часових рядів. Тип протоколу передачі інформації, а також тип переданої інформації (сервісна інформація, синхронізація, корисна інформація) ніяким чином не впливають на годину визначення коефіцієнта Херста. Він інваріантний до типів руйнівних впливів і не потребує налаштування або адаптації для виявлення конкретних типів атак, включаючи раніше невідомі. Разом з тим, слід зазначити, що збільшення кількості оброблюваних параметрів заголовка протоколу передачі даних (довжина пакета, прапорці тощо) призводить до збільшення години обчислення.

Запропонований інтегрований підхід, що поєднує фрактальний аналіз та машинне навчання для виявлення аномалій і кібернападів, має кілька унікальних переваг порівняно з традиційними методами.

По-перше, використання фрактального аналізу дозволяє виявляти складні закономірності та самоподібності в мережевому трафіку, які не завжди можна виявити за допомогою класичних методів. Це забезпечує раннє виявлення аномалій і кібернападів, що покращує безпеку мережі.

По-друге, використання моделей машинного навчання, зокрема рекурентних нейронних мереж, дозволяє ефективно розпізнавати складні аномалії і підвищує здатність виявляти нові типи загроз. Це дозволяє системі адаптуватися до змінюваних умов і виявляти навіть найскладніші кібернапади.

В цілому, інтеграція фрактального аналізу та машинного навчання створює потужний інструмент для виявлення аномалій і захисту мережі, що перевершує традиційні методи завдяки своїй унікальній здатності виявляти складні та еволюційні загрози.

Для підтвердження переваг було реалізовано фрагмент програмного коду, що використовує фрактальний аналіз і машинне навчання для виявлення аномалій у мережевому трафіку (рис. 9).

```
import numpy as np
import matplotlib.pyplot as plt
import tensorflow as tf
from tensorflow.keras.models import Sequential
from tensorflow.keras.layers import LSTM, Dense
from sklearn.preprocessing import MinMaxScaler

# Генерація синтетичних даних (мережевий трафік)
np.random.seed(0)
data = np.sin(np.linspace(0, 100, 1000)) + np.random.normal(0, 0.1, 1000)  # синусоїдальний трафік з шумом

# Функція для обчислення фрактальної вимірності
def fractal_dimension(signal):
    N = len(signal)
    box_sizes = np.logspace(1, np.log10(N//2), num=20)
    box_count = []
```

Рис. 9 Алгоритмічна схема інтеграції фрактального аналізу та машинного навчання для виявлення аномалій та кібератак

Джерело: побудовано авторами на основі проведених досліджень

У цьому коді ми використовували алгоритм ізоляційного лісу для виявлення аномалій у мережевому трафіку. Цей метод машинного навчання ґрунтується на ідеї, що аномальні спостереження є менш ймовірними, ніж нормальні. Після навчання моделі ми можемо робити прогнози на тестовій вибірці та оцінювати їх точність за допомогою звіту про класифікацію. Таким чином, цей код ілюструє використання машинного навчання для виявлення аномалій у мережевому трафіку, що є однією з переваг запропонованого підходу.

Висновки. В результаті аналізу таких досліджень можна зазначити, що багато робіт у сфері виявлення аномалій і кібернападів зосереджені на використанні специфічних методів, таких як машинне навчання, статистичні підходи або методи аналізу часових рядів. Водночас інтеграція фрактального аналізу з машинним навчанням для виявлення аномалій у кіберпросторі є новизною та додатковою перевагою. Це дослідження відрізняється здатністю враховувати складні залежності в даних за допомогою фрактального аналізу, що дозволяє виявляти не лише різкі сплески, але й повільні тренди, які можуть бути непоміченими в інших підходах. Крім того, інтеграція цього аналізу з методами машинного навчання, зокрема за допомогою гібридної штучної нейронної мережі, підвищує точність і надійність виявлення аномалій у реальному часі.

Література:

1. Види атак URL: https://www.geeksforgeeks.org/basic-network-attacks-in-computer-network/ (дата звернення: 25.10.2024)
2. Подвисоцька О.П., Носок С.О. *Застосування алгоритмів машинного навчання для виявлення аномалій мережного трафіку*. Теоретичні і прикладні проблеми фізики, математики та інформатики : матеріали XXII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених, [Київ], 13−17 травня 2024 р. / КПІ ім. Ігоря Сікорського. – Київ, 2024. – С. 288-290.
3. Розмір даних для виявлення аномалій без нагляду. URL: https://dataverse.harvard.edu/dataset.xhtml?persistentId=DOI:10.7910/DVN/OPQMVF (дата звернення: 15.11.2024)
4. Контрольні показники мета-аналізу виявлення аномалій. URL: https://ir.library.oregonstate.edu/concern/datasets/47429f155 (дата звернення: 20.11.2024)
5. R. F. Hodson, Real-Time Expert Systems Computer Architecture. *CRC Press*, 2018. p. 300. DOI: 10.1201/9781351076203.
6. R. S. Alford, Computer Systems Engineering Management. *CRC Press*, 2018. p. 392 DOI: 10.1201/9781351070829.
7. A. Yadin, Computer Systems Architecture, 1st ed. Boca Raton: *Taylor & Francis Group, CRC Press*, 2016. DOI: 10.1201/9781315373287.
8. I. Koren and C. M. Krishna, “Fault-Tolerant Networks,” in *Fault-Tolerant Systems*, Elsevier, 2021, pp. 115–159. DOI: 10.1016/B978-0-12-818105-8.00014-0.
9. Q. Hu, B. Xiao, B. Li, and Y. Zhang, “Fault-tolerant velocity-free attitude control,” in *Fault-Tolerant Attitude Control of Spacecraft*, Elsevier, 2021, pp. 125–173. DOI: 10.1016/B978-0-32-389863-8.00015-0.
10. S. X. Ding, “Performance Recovery and Fault-Tolerant Control Schemes,” in *Advanced methods for fault diagnosis and fault-tolerant control*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2021, pp. 553–600. DOI: 10.1007/978-3-662-62004-5_20.

References:

1. Types of Attacks o. Retrieved from: https://www.geeksforgeeks.org/basic-network-attacks-in-computer-network/
2. Podvysotska O.P., Nosok S.O. Zastosuvannia alhorytmiv mashynnoho navchannia dlia vyiavlennia anomalii merezhnoho trafiku [Application of machine learning algorithms for detecting anomalies in network traffic]. *Theoretical and Applied Problems of Physics, Mathematics, and Informatics: Proceedings of the XXII All-Ukrainian Scientific and Practical Conference of Students, Postgraduates, and Young Scientists*, [Kyiv], May 13–17, 2024 / Igor Sikorsky Kyiv Polytechnic Institute. – Kyiv, 2024. – P. 288-290.
3. Rozmir danykh dlia vyiavlennia anomalii bez nahliadu [Dataset Size for Unsupervised Anomaly Detection o]. Retrieved from: https://dataverse.harvard.edu/dataset.xhtml?persistentId=DOI:10.7910/DVN/OPQMVF.
4. Kontrolni pokaznyky meta-analizu vyiavlennia anomalii [Control Indicators for Anomaly Detection Meta-Analysis] Retrieved from: https://ir.library.oregonstate.edu/concern/ datasets/47429f155.
5. R. F. Hodson (2018) Real-Time Expert Systems Computer Architecture. *CRC Press*, 300. DOI: 10.1201/9781351076203 [in English].
6. R. S. Alford (2018). Computer Systems Engineering Management. *CRC Press*, 392 DOI: 10.1201/9781351070829 [in English].
7. A. Yadin (2016). Computer Systems Architecture, 1st ed. Boca Raton: Taylor & Francis Group, *CRC Press*, DOI: 10.1201/9781315373287 [in English].
8. I. Koren and C. M. Krishna (2021). Fault-Tolerant Networks, in Fault-Tolerant Systems, Elsevier, 115–159. DOI: 10.1016/B978-0-12-818105-8.00014-0 [in English].
9. Q. Hu, B. Xiao, B. Li, and Y. Zhang (2021) Fault-tolerant velocity-free attitude control, in Fault-Tolerant Attitude Control of Spacecraft, Elsevier, 125–173. DOI: 10.1016/B978-0-32-389863-8.00015-0 [in English].
10. S. X. Ding (2021). Performance Recovery and Fault-Tolerant Control Schemes, in Advanced methods for fault diagnosis and fault-tolerant control, Berlin, Heidelberg: *Springer Berlin Heidelberg*, 553–600. DOI: 10.1007/978-3-662-62004-5_20 [in English].

Журнал

«Наука і техніка сьогодні»

(Серія «Педагогіка», Серія «Право», Серія «Економіка», Серія «Фізико-математичні науки», Серія «Техніка»)

Випуск № 12(40) 2024

Формат 60х90/8. Папір офсетний.
Гарнітура Times New Roman.
Ум. друк. арк. 8,2. Наклад 100 прим.

Видавець:
Громадська наукова організація «Всеукраїнська асамблея докторів наук з державного управління»
Свідоцтво серія ДК №4957 від 18.08.2015 р., Андріївський узвіз, буд.11, оф 68, м. Київ, 04070.