КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (24), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.24.398414
УДК 004.056.5:004.896

**Іосіфов Євген Анатолійович**
аспірант кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID 0000-0001-6203-9945
*y.iosifov.asp@kubg.edu.ua*

**Соколов Володимир Юрійович**
к.т.н., доцент
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID 0000-0002-9349-7946
*v.sokolov@kubg.edu.ua*

# МЕТОДИ АНАЛІЗУ ПРИРОДНОЇ МОВИ ТА ЗАСТОСУВАННЯ НЕЙРОННИХ МЕРЕЖ В КІБЕРБЕЗПЕЦІ

**Анотація.** Робота підкреслює актуальність обробки природної мови (від англ. Natural Language Processing, NLP) у сучасному світі, зокрема через постійне зростання обсягів текстових даних у соціальних мережах, електронній комерції та онлайн-медіа. Автори зазначають, що ефективна обробка таких даних є критично важливою для бізнесу та державного управління, оскільки дозволяє генерувати нові знання, прогнозувати тренди та ухвалювати обґрунтовані рішення. NLP також робить вагомий внесок у підвищення ефективності роботи організацій за рахунок автоматизації обробки текстової інформації (наприклад, в системах підтримки клієнтів та аналізі відгуків). Крім цього, стаття наголошує на значних перспективах застосування NLP у сфері кібербезпеки. Зокрема, NLP використовується для автоматичного виявлення аномалій, моніторингу мережевого трафіку та виявлення фішингових атак. Для таких задач застосовуються глибинні моделі (наприклад, RNN, LSTM, CNN), а також новітні архітектури трансформерів, які здатні опрацьовувати великі обсяги інформації у реальному часі. Робота також порушує важливі питання, пов'язані з викликами сучасного NLP, серед яких — необхідність великих обчислювальних ресурсів, багатомовність, проблеми інтерпретації моделей та етичні аспекти, такі як упередженість та конфіденційність. На завершення, автори відзначають перспективи розвитку NLP, включно з дослідженням ефективніших алгоритмів для зменшення ресурсозатратності моделей, створенням більш інтерпретованих моделей, які зможуть пояснювати свої рішення, а також розробкою методів для підтримки низькоресурсних мов, що допоможе розширити використання NLP-технологій у глобальному масштабі. NLP є однією з найдинамічніших та найважливіших галузей штучного інтелекту, що дозволяє комп’ютерам розуміти, інтерпретувати та генерувати людську мову. У цій статті ми проводимо детальний огляд сучасних методів та технологій у сфері NLP, аналізуючи останні наукові статті та дослідження. Ми розглядаємо розвиток технологій, їх актуальність та новизну, а також глибоко аналізуємо проблематику та недоліки існуючих підходів. Окрім того, ми порівнюємо ефективність різних методів та надаємо рекомендації для майбутніх досліджень.

**Ключові слова:** обробка природної мови; глибинне навчання; трансформери; машинний переклад; аналіз емоцій; нейронні мережі; інтерпретованість; багатомовність; етичні аспекти; попередньо натреновані моделі; кібербезпека; інформаційна безпека.

## ВСТУП

Сучасні дослідження у сфері NLP характеризуються значними інноваціями, які суттєво впливають на розвиток штучного інтелекту, інформаційних технологій та кібербезпеки в цілому [1]. Новизна таких досліджень полягає в поєднанні передових

методів глибинного навчання з величезними обсягами доступних даних, що дозволяє створювати моделі, здатні вирішувати складні завдання, які раніше вважалися непідйомними.

Одним із найважливіших нововведень є використання попередньо натренованих моделей. Моделі такі як BERT (Bidirectional Encoder Representations from Transformers) та GPT (Generative Pre-trained Transformer) стали революційними у підході до вирішення NLP-завдань. Вони тренуються на масивних корпусах тексту, що дозволяє їм вивчати глибокі мовні закономірності та семантичні зв’язки між словами та фразами [2]. Це, в свою чергу, дає можливість ефективно адаптувати ці моделі до різноманітних прикладних задач без необхідності збору та анотування великих обсягів даних для кожної конкретної задачі. Такий підхід значно спрощує та прискорює процес розробки NLP-рішень, роблячи їх більш доступними та економічно вигідними для широкого кола користувачів та організацій.

Актуальність цих досліджень зумовлена кількома ключовими факторами, які впливають на різні аспекти суспільства та технологій. По-перше, безпрецедентне зростання обсягів текстових даних в епоху цифрової інформації створює нагальну потребу в ефективних методах їх обробки та аналізу. Соціальні мережі, електронна комерція, онлайн-медіа та інші цифрові платформи генерують величезні масиви текстової інформації щодня. Ефективна обробка цих даних є критично важливою для бізнесу, урядових організацій та наукової спільноти, оскільки вона дозволяє отримувати цінну інформацію, прогнозувати тенденції та приймати обґрунтовані рішення.

По-друге, потреба в автоматизації процесів стає все більш актуальною для підвищення ефективності та конкурентоспроможності організацій. Автоматизований аналіз відгуків клієнтів, модерація контенту, генерація звітів, обробка природної мови в системах підтримки клієнтів та багато інших завдань можуть бути виконані швидше та точніше за допомогою сучасних NLP-технологій. Це дозволяє зменшити витрати на ручну працю, мінімізувати людські помилки та покращити якість послуг.

По-третє, покращення взаємодії між людиною та комп'ютером є одним із головних пріоритетів сучасних технологій. Розвиток голосових асистентів, чат-ботів та інших інтерактивних систем, заснованих на NLP, робить взаємодію з технологіями більш природною та зручною. Це особливо важливо в контексті інклюзивних технологій, які надають доступ до інформації та сервісів людям з обмеженими можливостями, сприяючи соціальній інтеграції та рівності.

Крім того, сучасні дослідження у сфері NLP мають міждисциплінарний вплив, сприяючи розвитку таких галузей, як медицина, освіта, юриспруденція та інші. Наприклад, в медицині NLP використовується для аналізу медичних записів, виявлення симптомів та прогнозування захворювань, що може врятувати життя та покращити якість медичних послуг. В освіті технології NLP допомагають у створенні адаптивних навчальних систем, автоматичному оцінюванні робіт та наданні персоналізованого зворотного зв'язку студентам.

Таким чином, новизна та актуальність сучасних досліджень у сфері обробки природної мови визначаються їхнім значним впливом на технологічний прогрес, соціальний розвиток та економічне благополуччя. Подальший розвиток цих технологій обіцяє ще більші можливості та досягнення в майбутньому, відкриваючи нові перспективи для науки та суспільства в цілому.

Метою цієї статті є проведення всебічного огляду сучасних методів та підходів у сфері NLP, аналіз їх ефективності, а також виявлення актуальних проблем та напрямків

для подальших досліджень. Ми спираємося на ряд наукових статей, що висвітлюють різні аспекти NLP, щоб надати читачеві повне уявлення про поточний стан галузі.

**Постановка проблеми.** NLP стала невід'ємною частиною сучасних технологій, дозволяючи автоматизувати завдання, пов'язані з розумінням та генерацією людської мови. З появою інтернету та великих обсягів даних текстового формату потреба в ефективних методах обробки інформації стала критично важливою. NLP знайшла застосування у широкому спектрі галузей: від пошукових систем та соціальних мереж до медицини та фінансів. Останніми роками спостерігається значний прогрес у розвитку методів NLP, зокрема завдяки глибинному навчання та великим мовним моделям. Ці досягнення дозволяють вирішувати складні завдання, такі як машинне перекладання, автоматичне резюмування, аналіз сентименту, розпізнавання мови та багато інших. Недостатня увага до підходів розпізнавання природньої мови може призвести до застосування таких технологій у протиправній діяльності, що в свою чергу, призводить до збільшення ризиків успішних кібератак, особливо із застосуванням елементів соціальної інженерії, що є суттєвим для національної безпеки і безперервності ведення бізнесу [3].

**Аналіз останніх досліджень і публікацій.** Для проведення цього огляду було проаналізовано низку наукових статей, присвячених різним аспектам NLP. Вступ до глибинного навчання в NLP можна знайти в [4], а також в даному огляді описані основні задачі, інструменти та ресурси. Крім того, обговорюються обмеження поточних методів та майбутні напрямки розвитку. Також в [5] надається всебічний огляд компонентів NLP, історичного розвитку, основних застосувань, доступних датасетів, моделей та метрик оцінки. Вона акцентує увагу на поточних трендах та викликах, з якими стикається галузь. З іншого боку, глибинне навчання також застосовується в основних областях NLP, таких як мовне моделювання, морфологія, парсинг та семантика. Так [6] детально описує різні архітектури глибинного навчання та їх вплив на розвиток NLP.

Окремо розглядаються попередньо натреновані моделі для NLP, так в [7] приведена їхня класифікації та способах адаптації до прикладних задач, а також проаналізовані різні покоління попередньо натренованих моделей та їхній вплив на продуктивність при розв'язку різноманітних задач. В той самий час, у [8] обговорюється вплив глибинного навчання на різні задачі NLP, включаючи нові моделі та архітектури, переваги та недоліки глибинних методів порівняно з традиційними підходами. Окремо слід зазначити роль глибинного навчання у розвитку NLP, акцентуючи увагу на застосуваннях, викликах та досягненнях. Так в [9] розглядаються різні архітектури, такі як рекурентні нейронні мережі 'Recurrent Neural Networks' (RNN), згорткові нейронні мережі 'Convolutional Neural Networks' (CNN) та трансформери, а також їх вплив на продуктивність. З іншого боку, [10] надає огляд методів глибинного навчання та їх застосування у NLP, зокрема в задачах класифікації тексту, машинного перекладання, автоматичної корекції граматики та опису зображень.

Розглянуті в [11] ефективні методи в NLP, спрямовані на зменшення ресурсних витрат при збереженні або навіть покращенні продуктивності моделей, дозволяють виокремити виклики, пов'язані з великими обчислювальними витратами та способи їх подолання. Тому для вирішення цих викликів потрібно досліджувати застосування NLP у програмуванні, включаючи задачі, датасети та методи. Так стаття [12] акцентує увагу на особливостях програмних мов порівняно з природними мовами та методах їх обробки, а стаття [13] надає огляд різноманітних застосувань NLP, таких як класифікація тексту, іменоване розпізнавання сутностей, аналіз сентименту, машинне перекладання та розпізнавання мови. Розглядаються також виклики та майбутні напрямки досліджень.

## МЕТОДИКА ДОСЛІДЖЕННЯ

У статті обговорюються різноманітні методи обробки природної мови, зокрема ті, що мають важливе значення для розвитку NLP для розвитку кібербепеки. Основні методи і моделі, описані в роботі, включають: трансформерні моделі, моделі з механізмом уваги, попередньо натреновані моделі, архітектури рекурентних нейронних мереж, згорткові нейронні мережі, багатомодальні моделі, методи стиснення моделей і моделі на основі словникового представлення.

Об’єкт дослідження — розпізнавання небезпечних даних в системах забезпечення інформаційної безпеки. Предмет дослідження — методи, архітектури та технології для небезпечних даних в інформаційних системах.

## РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

### Розвиток технологій розпізнавання природньої мови

Розвиток NLP тісно пов’язаний з еволюцією методів машинного навчання, обчислювальних потужностей та доступності великих обсягів даних. В табл. 1 приведений історичний розвиток технологій NLP та ключові етапи, які привели галузь до сучасного стану.

*Таблиця 1*

**Етапи розвитку технології обробки природньої мови**

| Етапи | Роки | Опис |
|---|---|---|
| Ранні етапи розвитку | 1940-і — 1980-і | Перші спроби автоматизації обробки мови з’явилися у 1940-х роках, зосереджені на машинному перекладанні між мовами. Ці методи базувалися на простих системах, побудованих на правилах та статистичних підходах. У 1950-х роках з'явився термін «штучний інтелект», що стимулював дослідження в області розуміння мови. |
| Період машинного навчання | 1990-і — 2000-і | З розвитком комп’ютерних технологій та алгоритмів машинного навчання з'явилися більш просунуті методи обробки мови. Алгоритми, такі як приховані марковські моделі та умовні випадкові поля, стали популярними для задач розпізнавання мови та послідовного маркування. Використання статистичних методів дозволило обробляти великі обсяги даних та враховувати ймовірності переходів між станами. |
| Поява нейронних мереж та глибинного навчання | 2010-і | З початком 2010-х років глибинне навчання стало домінуючим підходом у багатьох областях, включаючи NLP. Моделі, такі як рекурентні нейронні мережі, довга короткочасна пам’ять та вентильний рекурентний вузол, були розроблені для вирішення проблеми зникання градієнтів та покращення обробки послідовних даних. У цей період також з’явилися методи словникових векторів, такі як Word2Vec та GloVe, що дозволили представляти слова у вигляді векторів, які відображають їх семантичні та синтаксичні відносини. |
| Революція трансформерів | з 2017 | У 2017 році була представлена архітектура трансформер, яка змінила підхід до обробки послідовностей. Трансформери використовують механізм уваги, що дозволяє моделі враховувати взаємозв'язки між будь-якими парами слів у послідовності, незалежно від їх віддаленості. Це призвело до появи потужних моделей, таких як BERT та GPT, які встановили нові стандарти в багатьох задачах NLP. |

| | | |
|---|---|---|
| Сучасний стан та майбутні перспективи | — | Сьогодні дослідження у сфері NLP зосереджені на покращенні моделей трансформерів, розробці ефективніших алгоритмів та розширенні застосувань на різні мови та домени. З'являються моделі з мільярдами параметрів, такі як GPT-3, які демонструють вражаючу здатність до генерації тексту, розуміння контексту та виконання складних завдань без спеціального навчання. |

Впровадження механізму уваги 'attention' стало ключовим фактором у підвищенні ефективності та точності моделей. Механізм уваги дозволяє моделі фокусуватися на важливих частинах вхідного тексту, враховуючи контекст та взаємозв'язки між словами незалежно від їх позиції у послідовності. Це особливо важливо для розуміння довгих та складних текстів, де традиційні рекурентні мережі могли втрачати інформацію через проблеми з довготривалими залежностями. Завдяки цьому, моделі на основі трансформерів здатні досягати кращих результатів у таких задачах, як машинне перекладання, автоматичне резюмування та відповідь на запити.

З іншого боку, архітектура трансформерів базується на механізмі уваги. Вони дозволяють моделі обробляти весь текст одночасно, що значно прискорює тренування та інференцію. Трансформери складаються з енкодерів та декодерів, які взаємодіють через механізм уваги.

Крім того, розвиток багатомодальних моделей відкриває нові горизонти для досліджень та застосувань. Поєднання NLP з іншими галузями, такими як комп'ютерний зір та обробка аудіо, призводить до створення моделей, здатних одночасно обробляти текст, зображення та звукові дані. Це дозволяє розробляти більш інтерактивні та інтуїтивні системи, такі як голосові асистенти, які можуть розуміти та реагувати на мовні та візуальні сигнали. Наприклад, моделі, здатні генерувати детальний опис зображень або відео на основі їх вмісту, можуть бути використані в додатках для людей з вадами зору або в системах автоматичного моніторингу та аналізу мультимедійного контенту.

Традиційні моделі (наївний баєсівський класифікатор, метод опорних векторів) прості, швидко тренуються та мають невисокі вимоги до ресурсів. Проте вони обмежені в здатності обробляти складні залежності та контекст. Натомість моделі глибинного навчання мають високу здатність до моделювання складних патернів та залежностей, а також можуть обробляти неструктуровані дані та виявляти нелінійні взаємозв'язки. Недоліки включають потребу в великих обсягах даних та обчислювальних ресурсів. Порівняння цих двох підходів приведено в табл. 2.

*Таблиця 2*

**Приклади архітектур попередньо натренованих моделей**

| Критерій | Традиційні статистичні моделі | Глибинне навчання |
|---|---|---|
| Складність моделей | відносно проста | висока |
| Обсяг даних для навчання | невеликий | значний |
| Попереднє опрацювання ознак | значна роль ручного відбору ознак | автоматичне виявлення ознак |
| Продуктивність на неструктурованих даних | обмежена | висока |
| Вимоги до обчислювальних ресурсів | низькі | високі |
| Інтерпретованість результатів | легка | складна |
| Час навчання моделі | швидкий | тривалий |
| Масштабованість | обмежена | висока |
| Здатність до узагальнення | залежить від моделі | висока (при правильному навчанні) |

| | | |
|---|---|---|
| Обробка нелінійних залежностей | обмежена | ефективна |
| Залежність від якості даних | висока | можуть компенсувати шум у даних |
| Підходить для високовимірних даних | менш ефективні | більш ефективні |
| Потреба в маркованих даних | може працювати з немаркованими | переважно потребує маркованих |
| Схильність до перенавчання | менша (при правильній регуляризації) | вища (але потребує методів запобігання) |
| Гнучкість у застосуванні | низька | висока |

## Проблематика сучасних досліджень у сфері обробки природньої мови

Можна виділити кілька основних напрямків перспективних досліджень:

– використання великих попередньо натренованих моделей, таких як BERT та GPT, дозволяє вирішувати різні задачі без потреби у великих обсягах мічених даних для кожної окремої задачі. Це стало можливим завдяки тренуванню на масивних корпусах тексту з використанням задач мовного моделювання;
– впровадження механізму уваги в моделях дозволяє ефективніше враховувати контекст та залежності між словами. Це особливо важливо для розуміння довгих послідовностей та складних структур мови;
– поєднання NLP з іншими галузями, такими як комп'ютерний зір, призвело до появи багатомодальних моделей, здатних обробляти текст разом з зображеннями або відео. Це відкриває нові можливості для задач, таких як опис зображень або відео.

Подальший розвиток таких систем обумовлений кількома факторами:

– з розвитком інтернету, соціальних мереж та цифрових медіа *обсяги доступної текстової інформації* стрімко зростають. Ефективна обробка та аналіз цих даних стають критично важливими;
– бізнес та інші сфери шукають способи *автоматизувати процеси*, пов'язані з обробкою тексту, такі як аналіз відгуків клієнтів, модерація контенту, автоматичне створення звітів тощо;
– розвиток NLP сприяє створенню більш природних та ефективних способів *взаємодії з комп'ютерами*, таких як голосові асистенти та чат-боти.

Незважаючи на значний прогрес, сфера NLP стикається з низкою серйозних проблем та викликів, які потребують подальших досліджень та рішень:

– моделям все ще складно повністю *зрозуміти контекстні нюанси*, іронію, сарказм та багатозначність слів;
– сучасні моделі, особливо ті, що базуються на трансформерах, є дуже *ресурсомісткими*. Тренування моделей з мільярдами параметрів вимагає потужних обчислювальних кластерів та значних енергетичних витрат. Це робить їх недоступними для багатьох дослідників та організацій з обмеженими ресурсами;
– більшість досліджень фокусується на англійській мові, що призводить до недостатньої підтримки інших мов, особливо тих, що мають *менше доступних даних*. Це обмежує можливості застосування NLP у глобальному масштабі та створює нерівність у доступі до технологій;
– глибинні моделі часто діють як «чорні скриньки», що ускладнює розуміння того, як і чому модель приймає певні рішення. Це може бути проблематичним у критичних застосуваннях, де важлива *прозорість* та можливість пояснити результати;
– використання NLP може призводити до *етичних проблем*, таких як упередженість моделей, порушення приватності, дезінформація та інші негативні наслідки. Наприклад, моделі можуть відтворювати та підсилювати соціальні упередження, якщо вони присутні у тренувальних даних.

**Порівняння сфер застосування різних типів нейронних мереж**

RNN спеціально розроблені для обробки послідовних даних, таких як текст або мовлення. Вони мають рекурентні зв'язки, що дозволяє їм зберігати інформацію про попередні елементи послідовності. Проте RNN страждають від проблеми зникання або вибуху градієнтів при довгих послідовностях. RNN добре підходять для обробки послідовних даних, таких як текст або аудіо, оскільки вони можуть враховувати часові залежності між елементами послідовності. Це робить їх ефективними для задач на кшталт розпізнавання мовлення або аналізу текстів, де важливо врахувати порядок слів або звуків.

Довга короткочасна пам'ять 'Long Short-Term Memory' (LSTM) — це тип RNN, що використовує спеціальні структури, звані «комірками пам'яті», які можуть зберігати інформацію протягом довгих періодів часу. Це дозволяє моделі ефективно обробляти довгі послідовності та враховувати контекст. LSTM розв'язує проблему короткострокової пам'яті та дозволяє моделі зберігати важливу інформацію впродовж довших часових проміжків. Завдяки цій особливості, LSTM є ефективними для складних задач, де необхідно зберігати залежності на довгій дистанції, наприклад, у машинному перекладі, розпізнаванні мовлення та генеруванні тексту.

Вентильний рекурентний вузол 'Gated Recurrent Unit' (GRU) це спрощена версія LSTM, що має менше параметрів та швидшу швидкість тренування. Вона також добре справляється з довгостроковими залежностями. GRU є спрощеною версією LSTM, яка зберігає більшу частину функціоналу, але має менше параметрів. GRU можуть бути ефективнішими з точки зору обчислень та швидкості навчання, і часто використовуються для задач обробки послідовностей, особливо коли ресурсів для тренування обмежено.

Хоча CNN традиційно використовуються у комп'ютерному зорі, вони також ефективні в NLP для задач класифікації тексту. CNN можуть виділяти локальні патерни та особливості, що є корисними для розпізнавання певних структур у тексті. CNN спроектовані для розпізнавання патернів у просторових даних, що робить їх надзвичайно ефективними для задач комп'ютерного бачення, таких як класифікація зображень та обробка відео. Проте CNN також застосовуються для текстових задач, таких як аналіз сентименту або класифікація тексту, де вони здатні захоплювати локальні залежності між словами або символами.

Таким чином, RNN, LSTM і GRU особливо ефективні в задачах обробки послідовностей, де важливі часові зв'язки, тоді як CNN демонструють високу ефективність у задачах, де ключовим є розпізнавання локальних патернів і просторових залежностей (див. табл. 3).

*Таблиця 3*

**Порівняння різних типів нейронних мереж**

| Критерій | RNN | LSTM | GRU | Трансформери |
|---|---|---|---|---|
| Здатність моделювати довгі залежності | обмежена через затухання градієнтів | висока завдяки коміркам пам'яті | висока, але з меншим числом параметрів | відмінна завдяки механізму уваги |
| Час навчання | швидкий | повільніший через складність | швидший за lstm | швидкий завдяки паралелізації |
| Обчислювальна ефективність | висока | нижча через більшу складність | краща за lstm | висока, але потребує більше пам'яті |
| Паралелізація | обмежена | обмежена | обмежена | відмінна |

| | | | | |
|---|---|---|---|---|
| Обробка послідовних даних | придатні | відмінно підходять | відмінно підходять | придатні, але безпосередньо не послідовні |
| Проблема затухання/вибуху градієнтів | схильні | менш схильні | менш схильні | не схильні |
| Вимоги до пам'яті | низькі | вищі через додаткові компоненти | нижчі за lstm | високі |
| Складність архітектури | проста | складна | помірна | складна |
| Підходять для задач | прості послідовності | довгі послідовності, мовні моделі | довгі послідовності, машинний переклад | мовні моделі, переклад, обробка тексту |
| Механізм уваги | відсутній | можна додати | можна додати | вбудований |
| Стан результатів | застарілі | актуальні | актуальні | сучасний стандарт |
| Обробка змінної довжини послідовностей | придатні | придатні | придатні | відмінно справляються |
| Інтерпретованість моделі | низька | нижча | нижча | вища завдяки увазі |
| Масштабованість | обмежена | обмежена | обмежена | висока |
| Легкість навчання | легко навчати | складніше навчати | легше за lstm | потребують багато даних та ресурсів |

RNN, LSTM, GRU добре обробляють послідовні дані, враховують порядок слів та короткострокові залежності. Проблеми виникають з довгими послідовностями та паралельною обробкою. В свою чергу, трансформери вирішують проблему довгострокових залежностей та дозволяють паралельно обробляти дані, що значно прискорює тренування. Проте вони можуть бути більш ресурсомісткими.

Продуктивність та швидкодія моделі є критичними факторами, особливо для застосувань у реальному часі, де важливий баланс між точністю та швидкістю. Для покращення продуктивності застосовують різні методи. Зокрема, прискорення обчислень здійснюється завдяки використанню графічних процесорів та тензорних блоків обробки, а також оптимізації коду. Стиснення моделей (див. в табл. 4 порівняльний аналіз), що включає прюнінг, квантізацію та дистиляцію знань, дозволяє зменшити розмір моделі без значної втрати точності. Крім того, паралельні обчислення, що передбачають розподіл обчислень на кілька пристроїв або серверів, допомагають підвищити швидкодію та ефективність роботи моделі.

*Таблиця 4*

**Приклади архітектур попередньо натренованих моделей**

| Абревіатура | Повна назва | Опис |
|---|---|---|
| BERT [14] | Bidirectional Encoder Representations from Transformers | BERT використовує двонапрямлене тренування, що дозволяє моделі враховувати контекст з обох сторін від слова. Це покращує розуміння семантики та контексту. BERT показує високі результати у різних задачах, таких як класифікація, розпізнавання іменованих об’єктів та питання-відповідь. |
| GPT [15] | Generative Pre-trained Transformer | Генеративна модель, що фокусується на прогнозуванні наступного слова у послідовності. GPT-4, зокрема, має понад |

| | | |
|---|---|---|
| | | 175 мільярдів параметрів та здатна виконувати широкий спектр задач без спеціального навчання. |
| RoBERTa [16] | — | Оптимізована версія BERT, що використовує вдосконалені методи тренування, такі як більший обсяг даних та довший час тренування. Вона демонструє покращену продуктивність у порівнянні з оригінальним BERT. |
| XLNet [17] | — | Модель, що поєднує переваги автогресивних моделей (таких як GPT) та двонапрямлених моделей (таких як BERT). Вона використовує пермутоване мовне моделювання для врахування всіх можливих порядків слів. |

**Порівняння загальних сфер застосування різних типів нейронних мереж**

Ефективність нейронних мереж у різних задачах варіюється залежно від їхньої архітектури та особливостей задачі. Можна виділити кілька типових задач:

- трансформери показують найкращі результати в *машинному перекладі* завдяки механізму уваги, який дозволяє обробляти довгі залежності в тексті. Завдяки цьому трансформери можуть розуміти контекст як на рівні речень, так і на рівні абзаців, що робить їх ідеальними для складного та точного перекладу текстів;
- CNN можуть бути ефективними для швидкої класифікації тексту завдяки здатності виявляти локальні патерни, наприклад, *емоційні тригери* або *ключові фрази* [18]. У задачах аналізу сентименту CNN здатні швидко й точно класифікувати настрої в тексті, зокрема в соціальних мережах або відгуках клієнтів;
- RNN та їхні розширення, такі як LSTM, чудово справляються з послідовностями аудіо даних, адже можуть запам'ятовувати довготривалі залежності у часових рядах. Ці моделі ефективно використовуються для автоматичного *розпізнавання мовлення*, оскільки враховують послідовність звуків і вимов, що важливо для розуміння природної мови;
- LSTM і GRU підходять для задач розпізнавання *іменованих сутностей*, оскільки вони можуть враховувати контекст навколо кожного слова в тексті та визначати, чи є воно сутністю, наприклад, ім’ям, локацією або організацією. Також використовується комбінація LSTM з механізмом уваги, що дозволяє підвищити точність, особливо у великих текстах;
- CNN є стандартом для задач *класифікації зображень*, оскільки здатні ефективно виявляти патерни, форми та текстури в піксельних даних. Завдяки цьому CNN використовуються для ідентифікації об'єктів у зображеннях, діагностики медичних знімків, аналізу супутникових даних та розпізнавання облич;
- RNN, LSTM і GRU ефективні для задач прогнозування в *тимчасових рядах*, оскільки зберігають інформацію про попередні стани, що дозволяє прогнозувати майбутні значення. Ці архітектури активно використовуються в фінансовому прогнозуванні, моніторингу клімату та аналізі промислових процесів;
- трансформери, зокрема їхні варіанти, такі як GPT, є ефективними для *генерації тексту* завдяки здатності розуміти та підтримувати контекст на великій дистанції. Ці моделі використовуються для створення креативних текстів, автоматичного заповнення, діалогових систем та чат-ботів, здатних відповідати на складні запити;
- задачі *аналізу відео* часто поєднують CNN для обробки просторової інформації (кожного кадру) з LSTM або GRU, які обробляють часові залежності між кадрами. Такий підхід використовується для розпізнавання дій, детекції аномалій у відео та автоматизації процесів, де важливо враховувати послідовність подій.

Попередньо натреновані моделі показують високі результати у багатьох задачах, але вимагають значних ресурсів для тренування. Тому для ефективного використання обчислювальних ресурсів краще застосовувати різні архітектури нейронних мереж для

вирішення специфічних завдань, особливо має свою нішу застосування, де її особливості дозволяють досягати найкращих результатів у задачах на кшталт обробки тексту, аналізу зображень або прогнозування на основі тимчасових рядів.

**Порівняння загальних сфер застосування різних типів нейронних мереж**

З іншого боку для вирішення задач, пов'язаних із забезпеченням кібербезпеки, можна виділити ряд напрямків, в яких застосування відповідних моделей нейронних мереж може дати виграш у швидкості реагування на загрози та інциденти:

1. Виявлення *незвичайної або підозрілої активності* (аномалій) в мережевому трафіку, що може свідчити про кібератаки, вторгнення або витік даних (автоенкодери, RNN, LSTM та GRU).
2. Ідентифікація та класифікація *шкідливого програмного забезпечення* на основі коду, поведінки або мережевої активності (ефективні CNN та графові нейронні мережі).
3. Розпізнавання *фішингових* електронних листів, веб-сайтів або повідомлень, які намагаються отримати конфіденційну інформацію (трансформери, BiLSTM та CNN).
4. Обробка великих обсягів *лог-файлів* для виявлення підозрілої активності та інцидентів безпеки (RNN та моделі уваги).
5. *Моніторинг мережі* для виявлення несанкціонованих дій, в тому числі системи виявлення вторгнень (глибокі нейронні мережі, автоенкодери та CNN).
6. Виявлення *аномалій у поведінці користувачів* (так зване UBA) для запобігання зловмисним діям. Використовуються моделі машинного навчання з підкріпленням та LSTM.
7. Виявлення та блокування небажаних та шкідливих повідомлень і *спаму* в ширшому сенсі (наївний баєсівський класифікатор, метод опорних векторів, CNN та трансформери).
8. Ідентифікація *мереж заражених пристроїв* та інших ботнетів (графові нейронні мережі та автоенкодери).
9. Виявлення потенційних *уразливостей* у програмному забезпеченні та експлойтів (GNN та трансформери).
10. Передбачення майбутніх кібератак на основі *історичних даних* (моделі часових рядів та LSTM).
11. Використання біометричних даних для захисту доступу (CNN та RNN).
12. Виявлення та пом'якшення атак типу «*відмова в обслуговуванні*»: DoS і DDoS (CNN, RNN та моделі кластеризації).
13. Виявлення *нелегальної активності* на «темних» веб-ресурсах (моделі NLP та трансформери).
14. Виявлення шкідливої активності у *зашифрованому трафіку* без розшифрування (моделі статистичного аналізу та CNN).
15. Автоматичне виявлення та реагування на *інциденти безпеки* (моделі машинного навчання з підкріпленням.

Використання цих моделей може значно підвищити ефективність виявлення та реагування на загрози, дозволяючи адаптуватися до нових атак та автоматизувати процеси захисту, а також сигналізувати офіцерам безпеки про виявленні та потенційні загрози [19-21].

**Методи словникового подання для боротьби зі спамом**

Можна також виділити для забезпечення навчання антиспам систем методи словникового подання, наприклад, Word2Vec, GloVe та інші. Так Word2Vec — це набір моделей, розроблених для отримання векторних представлень слів. До нього входять основні архітектури: прогнозування слова за його контекстом (Continuous Bag of Words) та контекстного слова за заданим словом (Skip-Gram). Ці моделі вчаться на великих корпусах тексту та створюють вектори, де семантично схожі слова розташовані близько один до одного у векторному просторі. Метод GloVe (Global Vectors) поєднує глобальну матрицю співвідношень слів та локальний контекст, щоб отримати більш точні векторні представлення. GloVe враховує глобальні статистики корпусу, що дозволяє краще відображати рідкісні слова. А FastText (розширення Word2Vec) враховує морфологію слів, представляючи кожне слово як набір символів або n-грам. Це покращує представлення рідкісних та складених слів.

**Підходи до визначення ефективності застосування нейронних мереж**

BLEU, ROUGE, і F1-score — це три різні метрики, що використовуються для оцінки якості алгоритмів природної мови, але кожна з них має специфічне призначення і підходить для різних типів задач.

Метрика BLEU (від. Bilingual Evaluation Understudy) застосовується в основному для оцінки якості машинного перекладу. Вона порівнює автоматичний переклад із набором еталонних перекладів, обчислюючи, наскільки добре перекладений текст відповідає реальному тексту. Ця метрика найбільше підходить для задач, де важливо порівняти точність і контекст відповідності між машинним і людським перекладом.

ROUGE (від. Recall-Oriented Understudy for Gisting Evaluation), навпаки, використовується для оцінки якості автоматичного резюмування. Вона зосереджена на повноті (recall), вимірюючи, наскільки добре важливі частини еталонного резюме представлені в автоматично згенерованому резюме. ROUGE часто використовується у задачах, де важливо оцінити змістовність і адекватність стисненого тексту.

F1-score, який комбінує точність (precision) та повноту (recall), використовується в задачах класифікації та розпізнавання іменованих сутностей. Він балансує між точністю, яка відображає, наскільки добре алгоритм передбачає правильні метки, і повнотою, яка показує, наскільки повно він охоплює всі очікувані метки.

Отже, BLEU підходить для оцінки якості машинного перекладання шляхом порівняння з еталонними перекладами, ROUGE для автоматичного резюмування, а F1-score — для задач класифікації та розпізнавання іменованих сутностей, де важливо підтримувати баланс між точністю та повнотою.

Баланс між точністю та швидкістю моделі є критичним, особливо для застосувань в реальному часі. Для покращення продуктивності використовуються методи: прискорення обчислень, стиснення моделей і паралельних обчислень.

**Перспективи використання сучасних архітектур у сфері кібербезпеки**

У сучасному цифровому просторі, де обсяг інформації та складність кіберзагроз постійно зростають, кібербезпека стає одним із найважливіших напрямів досліджень та практичного застосування. Сучасні технології NLP та GPT-архітектури відкривають нові можливості для виявлення, аналізу та запобігання кіберзагрозам, що робить їх актуальними для використання в цій сфері.

Інтеграція сучасних NLP та GPT-архітектур у сферу кібербезпеки є новим та актуальним напрямом, що пропонує значні переваги у боротьбі з кіберзагрозами. Ці технології дозволяють глибше розуміти та аналізувати текстову інформацію, виявляючи складні патерни та аномалії. Однак для максимально ефективного їх використання необхідно вирішувати існуючі виклики та забезпечувати етичне та правове обґрунтування їх застосування.

Традиційні методи кібербезпеки часто базуються на сигнатурному аналізі та правилових підходах, які не завжди здатні ефективно виявляти нові або модифіковані загрози. Сучасні NLP-моделі, зокрема ті, що базуються на GPT-архітектурах, здатні аналізувати великі обсяги текстових даних та виявляти складні патерни, які можуть вказувати на потенційні загрози.

Новизна цих підходів полягає у використанні глибокого навчання та трансформерних моделей для обробки природної мови, що дозволяє системам розуміти контекст та семантику тексту на більш високому рівні. Це особливо корисно для:

- виявлення фішингових атак (GPT-моделі можуть аналізувати електронні листи та повідомлення, виявляючи нетипові мовні конструкції та зміст, що характерні для фішингу);
- аналізу шкідливого програмного забезпечення (розуміння коду та коментарів у шкідливих програмах допомагає у їх швидкому виявленні та нейтралізації);
- моніторингу темних веб-ресурсів (NLP може використовуватися для аналізу дискусій та повідомлень на форумах, де кіберзлочинці обмінюються інформацією).

Зі зростанням кількості кібератак та їх складності, традиційні методи захисту стають менш ефективними. Сучасні NLP та GPT-моделі здатні адаптуватися до нових загроз завдяки своїй архітектурі та можливості навчатися на великих наборах даних. Це робить їх незамінними у таких аспектах:

- можуть оперативно аналізувати нову інформацію та оновлювати свої алгоритми виявлення;
- можуть бути налаштовані під специфічні потреби організації, враховуючи унікальні патерни поведінки та потенційні ризики;
- дозволяють автоматизувати багато рутинних задач, зменшуючи навантаження на аналітиків та підвищуючи ефективність роботи.

Незважаючи на значні переваги, використання сучасних NLP та GPT-архітектур у кібербезпеці має ряд викликів:

- для ефективного навчання моделей необхідні великі набори даних, що можуть бути недоступними або конфіденційними;
- ті ж самі моделі можуть бути використані кіберзлочинцями для створення більш переконливих фішингових атак або шкідливого контенту;
- обробка персональних даних вимагає дотримання законодавства про конфіденційність та захист інформації.

## ЗАСТОСУВАННЯ ОБРОБКИ ПРИРОДНОЇ МОВИ В СФЕРІ КІБЕРБЕЗПЕКИ

Сьогодні дослідження у сфері NLP зосереджені на покращенні моделей трансформерів, розробці ефективніших алгоритмів та розширенні застосувань на різні мови та домени. З’являються моделі з мільярдами параметрів, такі як Claude Sonnet та GPT-4, які демонструють вражаючу здатність до генерації тексту, розуміння контексту та виконання складних завдань без спеціального навчання.

NLP відіграє кілька важливих ролей у сучасній кібербезпеці. Вдосконалені алгоритми NLP можуть аналізувати шаблони в текстових повідомленнях, щоб виявити

потенційні спроби фішингу, визначаючи підозрілі мовні шаблони, незвичні запити або тактики соціальної інженерії. Команди безпеки використовують NLP для автоматичної обробки та категоризації журналів безпеки та сповіщень, що допомагає їм визначати пріоритети та ефективніше реагувати на загрози [22].

Також NLP дає змогу аналізувати настрої комунікацій у темному інтернеті, щоб виявляти нові загрози та відстежувати діяльність кіберзлочинців. Завдяки класифікації тексту та виявленню аномалій NLP допомагає ідентифікувати підозрілі послідовності команд та потенційні спроби виконання шкідливого коду. Системи на основі NLP можуть відстежувати внутрішні комунікації на предмет потенційного витоку даних або внутрішніх загроз, відзначаючи незвичні шаблони спілкування або несанкціонований обмін конфіденційною інформацією.

Чат-боти з NLP можуть забезпечити негайне реагування першого рівня на інциденти безпеки та провести користувачів через протоколи безпеки. Методи NLP допомагають аналізувати описи шкідливих програм і звіти про загрози, щоб виявити схожість між новими і відомими загрозами, допомагаючи в розвідці загроз. Обробляючи запити природною мовою, NLP робить документацію з безпеки та бази знань більш доступними для команд безпеки під час реагування на інциденти [23].

Аналіз мережевого трафіку виграє від NLP завдяки виявленню командно-контрольних комунікацій і спроб витоку даних, прихованих у трафіку, що виглядає легітимно. Системи захисту електронної пошти використовують NLP для виявлення спаму, спроб компрометації ділової електронної пошти та складних фішингових кампаній. Вдосконалені моделі NLP можуть аналізувати коментарі до коду та документацію, щоб виявити потенційні вразливості безпеки під час процесу розробки.

Дотримання політики безпеки можна автоматизувати, використовуючи NLP для сканування документів і повідомлень на предмет потенційних порушень. NLP допомагає обробляти та співвідносити дані про загрози з різних джерел для створення комплексних оцінок загроз. Можливості генерації природної мови допомагають створювати автоматизовані звіти та оповіщення про безпеку, які є більш зрозумілими та зручними для команд безпеки. Аналізуючи взаємодію з людиною, NLP може виявити спроби несанкціонованого доступу або незвичайні моделі поведінки, які можуть свідчити про компрометацію.

Тренінги з підвищення обізнаності про безпеку виграють від NLP завдяки персоналізованій подачі контенту та оцінці розуміння користувачами. Системи на основі NLP можуть автоматично генерувати і підтримувати документацію з безпеки, обробляючи звіти про інциденти і процедури реагування. Полювання на загрози стає більш ефективним, оскільки NLP допомагає аналітикам швидко обробляти і співвідносити величезні обсяги неструктурованих даних про безпеку. Системи розпізнавання голосу, вдосконалені за допомогою NLP, можуть додати додатковий рівень безпеки для голосових систем і виявляти потенційні голосові атаки.

Нарешті, актуальність досліджень у сфері NLP підкріплюється економічними вигодами. Інвестиції в технології NLP можуть привести до значного економічного зростання, створення нових робочих місць та підвищення продуктивності в різних секторах економіки. Компанії, що впроваджують передові NLP-рішення, отримують конкурентні переваги, можуть пропонувати інноваційні продукти та послуги, задовольняючи зростаючі потреби ринку.

## ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Глобалізація та міжкультурна комунікація виграють від розвитку NLP. Системи автоматичного перекладу дозволяють долати мовні бар'єри, сприяючи обміну знаннями, культурою та бізнес-можливостями між країнами та регіонами. Це особливо актуально в сучасному світі, де міжнародна співпраця та комунікація є ключовими факторами успіху.

Як видно із розглянутих джерел обробка природної мови продовжує активно розвиватися завдяки глибинному навчання та новим моделям, таким як трансформери. Ці досягнення відкривають нові можливості для автоматизації та покращення різних задач, пов'язаних з розумінням та генерацією мови.

Проте існують серйозні виклики, пов'язані з ресурсомісткістю моделей, багатомовністю, інтерпретованістю та етичними аспектами, тому для подальшого розвитку та впровадження NLP технологій необхідно:

- розроблювати ефективніші алгоритми та архітектури, що зменшують потребу в обчислювальних ресурсах (наприклад, використання знань дистиляції, прюнінгу та квантізації);
- розширювати дослідження на інші мови, особливо ті, що мають обмежені ресурси, та використовувати методи переносу знань та багатомовних моделей;
- покращувати розуміння внутрішніх механізмів моделей для підвищення довіри та можливості пояснити результати та розроблювати інструменти для візуалізації та аналізу рішень моделей;
- врахувати приватності, упередженості та інших етичних питань при розробці та впровадженні NLP технологій і встановлювати стандарти та практики для відповідального використання штучного інтелекту;
- розроблювати методи, що дозволяють використовувати NLP технології на пристроях з обмеженими ресурсами, таких як мобільні телефони або IoT пристрої.

В якості наступних досліджень можна виділити забезпечення підтримки низькоресурсних мов через розширення ресурсів, таких як корпуси та моделі, а також використання методів переносу навчання та багатомовних моделей.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Iosifova, O., Iosifov, I., Rolik, O., & Sokolov, V. (2020). Techniques Comparison for Natural Language Processing. In *Proceedings of the 2nd International Workshop on Modern Machine Learning Technologies and Data Science* (No. I, vol. 2631, pp. 57–67).
2. Iosifova, O., Iosifov, I., Sokolov, V., Romanovskyi, O., & Sukaylo, I. (2021). Analysis of Automatic Speech Recognition Methods. In *Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems* (Vol. 2923, pp. 252–257).
3. Iosifov, I. Iosifova, O., Sokolov, V., Skladannyi, P., & Sukaylo, I. (2021). Natural Language Technology to Ensure the Safety of Speech Information. In *Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems II* (Vol. 3187, no. 1, pp. 216–226).
4. Lauriola, I., Lavelli, A., & Aiolli, F. (2021). An Introduction to Deep Learning in Natural Language Processing: Models, Techniques, and Tools. *Neurocomputing* (Vol. 470, pp. 443–456). https://doi.org/10.1016/j.neucom.2021.05.103.
5. Khurana, D., Koli, A., Khatter, K., & Singh, S. (2017). Natural Language Processing: State of the Art, Current Trends and Challenges. *Multimedia Tools and Applications* (Vol. 82, pp. 3713–3744). https://doi.org/10.1007/s11042-022-13428-4.
6. Otter, D., Medina, J., & Kalita, J. (2020). A Survey of the Usages of Deep Learning for Natural Language Processing. *IEEE Transactions on Neural Networks and Learning Systems* (Vol. 32, pp. 604–624). https://doi.org/10.1109/TNNLS.2020.2979670.

7. Qiu, X., Sun, T., Xu, Y., Shao, Y., Dai, N., & Huang, X. (2020). Pre-Trained Models for Natural Language Processing: A Survey. *Science China Technological Sciences* (Vol. 63, pp. 1872–1897). https://doi.org/10.1007/s11431-020-1647-3.
8. Zhang, J., & Zong, C. (2019). Deep Learning for Natural Language Processing. *Cognitive Computation Trends*. https://doi.org/10.1007/978-3-030-06073-2_5.
9. Torfi, A., Shirvani, R., Keneshloo, Y., Tavvaf, N., & Fox, E. (2020). Natural Language Processing Advancements by Deep Learning: A Survey. *arXiv* (pp. 1–23). https://doi.org/10.48550/arXiv.2003.01200.
10. Yang, H., Luo, L., Chueng, L., Ling, D., & Chin, F. (2019). Deep Learning and Its Applications to Natural Language Processing. *Cognitive Computation Trends*. https://doi.org/10.1007/978-3-030-06073-2_4.
11. Treviso, M., Ji, T., Lee, J., Aken, B., Cao, Q., Ciosici, M., Hassid, M., Heafield, K., Hooker, S., Martins, P., Martins, A., Milder, P., Raffel, C., Simpson, E., Slonim, N., Balasubramanian, N., Derczynski, L., & Schwartz, R. (2022). Efficient Methods for Natural Language Processing: A Survey. *Transactions of the Association for Computational Linguistics* (Vol. 11, pp. 826–860). https://doi.org/10.1162/tacl_a_00577.
12. Zhu, Q., Luo, X., Liu, F., Gao, C., & Che, W. (2022). A Survey on Natural Language Processing for Programming. *arXiv* (pp. 1–13). https://doi.org/10.48550/arXiv.2212.05773.
13. Dande, A., & Pund, D. (2023). A Review Study on Applications of Natural Language Processing. *International Journal of Scientific Research in Science, Engineering and Technology*. https://doi.org/10.32628/ijsrset2310214.
14. Devlin, J., Chang, M.-W., Lee, K., & Toutanova, K. (2019). BERT: Pre-Training of Deep Bidirectional Transformers for Language Understanding. In *Proceedings of the Conference of the North. Association for Computational Linguistics* (pp. 1–16). https://doi.org/10.18653/v1/n19-1423.
15. Issaiy, M., Ghanaati, H., Kolahi, S., Shakiba, M., Jalali, A. H., Zarei, D., Kazemian, S., Avanaki, M. A., & Firouznia, K. (2024). Methodological insights into ChatGPT's Screening Performance in Systematic Reviews. In *BMC Medical Research Methodology* (Vol. 24, no. 1). https://doi.org/10.1186/s12874-024-02203-8.
16. Liu, Y., Ott, M., Goyal, N., Du, J., Joshi, M., Chen, D., Levy, O., Lewis, M., Zettlemoyer, L., & Stoyanov, V. (2019). RoBERTa: A Robustly Optimized BERT Pretraining Approach. *arXiv* (pp. 1–13). https://doi.org/10.48550/arXiv.1907.11692.
17. Yang, Z., Dai, Z., Yang, Y., Carbonell, J., Salakhutdinov, R., & Le, Q. V. (2019). XLNet: Generalized Autoregressive Pretraining for Language Understanding. In *Proceedings of the 33rd International Conference on Neural Information Processing Systems* (Article 517, pp. 5753–5763).
18. Iosifov, I., Iosifova, O., Romanovskyi, O., Sokolov, V., & Sukailo, I. (2022). Transferability Evaluation of Speech Emotion Recognition between Different Languages. In *Lecture Notes on Data Engineering and Communications Technologies* (pp. 413–426). https://doi.org/10.1007/978-3-031-04812-8_35.
19. K. Khorolska, et al., (2022) Application of a Convolutional Neural Network with a Module of Elementary Graphic Primitive Classifiers in the Problems of Recognition of Drawing Documentation and Transformation of 2D to 3D Models, J. Theor. Appl. Inf. Technol. 100(24) 7426–7437
20. Korshun, N., Myshko, I., & Tkachenko, O. (2023). Automation and Management in Operating Systems: The Role of Artificial Intelligence and Machine Learning. In 20th International Scientific Conference "Dynamical System Modeling and Stability Investigation" (DSMSI), Volume 1: Mathematical Foundations of Information Technologies (vol. 3687, pp. 59–68)
21. V. Buhas, et al., (2024) AI-Driven Sentiment Analysis in Social Media Content, in: Workshop on Digital Economy Concepts and Technologies Workshop, DECaT, vol. 3665 12–21
22. Sukaylo, I., & Korshun, N. (2022). THE Influence of NLU and Generative AI on the Development of Cyber Defense Systems. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, *2*(18), 187–196. https://doi.org/10.28925/2663-4023.2022.18.187196
23. D. Shevchuk, et al., (2023) Designing Secured Services for Authentication, Authori-zation, and Accounting of Users, in: Cybersecurity Providing in Information and Telecommunication Systems II Vol. 3550 217–225.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (24), 2024
ISSN 2663 - 4023

**Ievgen A. Iosifov**
Ph.D. student of Volodymyr Buriachok Department of Information and Cybersecurity
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID 0000-0001-6203-9945
*y.iosifov.asp@kubg.edu.ua*

**Volodymyr Y. Sokolov**
Ph.D., associate professor
associate professor of Volodymyr Buriachok Department of Information and Cybersecurity
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID 0000-0002-9349-7946
*v.sokolov@kubg.edu.ua*

# METHODS OF NATURAL LANGUAGE ANALYSIS USING NEURAL NETWORKS IN CYBER SECURITY

**Abstract.** The work emphasizes the relevance of natural language processing (NLP) in the modern world, in particular due to the constant growth of text data in social networks, e-commerce and online media. The authors note that the effective processing of such data is critically important for business and public administration, as it allows generating new knowledge, predicting trends and making informed decisions. NLP also makes a significant contribution to improving the efficiency of organizations by automating the processing of text information (for example, in customer support systems and feedback analysis). In addition, the article emphasizes the significant prospects for the application of NLP in the field of cybersecurity. In particular, NLP is used for automatic anomaly detection, network traffic monitoring and detection of phishing attacks. For such tasks, deep models (for example, RNN, LSTM, CNN) are used, as well as the latest transformer architectures that are capable of processing large amounts of information in real time. The work also raises important questions related to the challenges of modern NLP, including the need for large computational resources, multilingualism, model interpretation issues, and ethical aspects such as bias and privacy. Finally, the authors note the prospects for the development of NLP, including the study of more efficient algorithms to reduce the resource consumption of models, the creation of more interpretable models that can explain their decisions, as well as the development of methods to support low-resource languages, which will help expand the use of NLP technologies on a global scale. NLP is one of the most dynamic and important branches of artificial intelligence, which allows computers to understand, interpret, and generate human language. In this article, we conduct a detailed review of modern methods and technologies in the field of NLP, analyzing the latest scientific articles and research. We consider the development of technologies, their relevance and novelty, and also deeply analyze the problems and shortcomings of existing approaches. In addition, we compare the effectiveness of different methods and provide recommendations for future research.

**Keywords:** Natural Language Processing; deep learning; transformers; machine translation; emotion analysis; neural networks; interpretability; multilingualism; ethical aspects; pre-trained models; cybersecurity; information security.

## REFERENCES

1. Iosifova, O., Iosifov, I., Rolik, O., & Sokolov, V. (2020). Techniques Comparison for Natural Language Processing. In *Proceedings of the 2nd International Workshop on Modern Machine Learning Technologies and Data Science* (No. I, vol. 2631, pp. 57–67).
2. Iosifova, O., Iosifov, I., Sokolov, V., Romanovskyi, O., & Sukaylo, I. (2021). Analysis of Automatic Speech Recognition Methods. In *Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems* (Vol. 2923, pp. 252–257).
3. Iosifov, I. Iosifova, O., Sokolov, V., Skladannyi, P., & Sukaylo, I. (2021). Natural Language Technology to Ensure the Safety of Speech Information. In *Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems II* (Vol. 3187, no. 1, pp. 216–226).
4. Lauriola, I., Lavelli, A., & Aiolli, F. (2021). An Introduction to Deep Learning in Natural Language Processing: Models, Techniques, and Tools. *Neurocomputing* (Vol. 470, pp. 443–456). https://doi.org/10.1016/j.neucom.2021.05.103.

5. Khurana, D., Koli, A., Khatter, K., & Singh, S. (2017). Natural Language Processing: State of the Art, Current Trends and Challenges. *Multimedia Tools and Applications* (Vol. 82, pp. 3713–3744). https://doi.org/10.1007/s11042-022-13428-4.
6. Otter, D., Medina, J., & Kalita, J. (2020). A Survey of the Usages of Deep Learning for Natural Language Processing. *IEEE Transactions on Neural Networks and Learning Systems* (Vol. 32, pp. 604–624). https://doi.org/10.1109/TNNLS.2020.2979670.
7. Qiu, X., Sun, T., Xu, Y., Shao, Y., Dai, N., & Huang, X. (2020). Pre-Trained Models for Natural Language Processing: A Survey. *Science China Technological Sciences* (Vol. 63, pp. 1872–1897). https://doi.org/10.1007/s11431-020-1647-3.
8. Zhang, J., & Zong, C. (2019). Deep Learning for Natural Language Processing. *Cognitive Computation Trends*. https://doi.org/10.1007/978-3-030-06073-2_5.
9. Torfi, A., Shirvani, R., Keneshloo, Y., Tavvaf, N., & Fox, E. (2020). Natural Language Processing Advancements by Deep Learning: A Survey. *arXiv* (pp. 1–23). https://doi.org/10.48550/arXiv.2003.01200.
10. Yang, H., Luo, L., Chueng, L., Ling, D., & Chin, F. (2019). Deep Learning and Its Applications to Natural Language Processing. *Cognitive Computation Trends*. https://doi.org/10.1007/978-3-030-06073-2_4.
11. Treviso, M., Ji, T., Lee, J., Aken, B., Cao, Q., Ciosici, M., Hassid, M., Heafield, K., Hooker, S., Martins, P., Martins, A., Milder, P., Raffel, C., Simpson, E., Slonim, N., Balasubramanian, N., Derczynski, L., & Schwartz, R. (2022). Efficient Methods for Natural Language Processing: A Survey. *Transactions of the Association for Computational Linguistics* (Vol. 11, pp. 826–860). https://doi.org/10.1162/tacl_a_00577.
12. Zhu, Q., Luo, X., Liu, F., Gao, C., & Che, W. (2022). A Survey on Natural Language Processing for Programming. *arXiv* (pp. 1–13). https://doi.org/10.48550/arXiv.2212.05773.
13. Dande, A., & Pund, D. (2023). A Review Study on Applications of Natural Language Processing. *International Journal of Scientific Research in Science, Engineering and Technology*. https://doi.org/10.32628/ijsrset2310214.
14. Devlin, J., Chang, M.-W., Lee, K., & Toutanova, K. (2019). BERT: Pre-Training of Deep Bidirectional Transformers for Language Understanding. In *Proceedings of the Conference of the North. Association for Computational Linguistics* (pp. 1–16). https://doi.org/10.18653/v1/n19-1423.
15. Issaiy, M., Ghanaati, H., Kolahi, S., Shakiba, M., Jalali, A. H., Zarei, D., Kazemian, S., Avanaki, M. A., & Firouznia, K. (2024). Methodological insights into ChatGPT's Screening Performance in Systematic Reviews. In *BMC Medical Research Methodology* (Vol. 24, no. 1). https://doi.org/10.1186/s12874-024-02203-8.
16. Liu, Y., Ott, M., Goyal, N., Du, J., Joshi, M., Chen, D., Levy, O., Lewis, M., Zettlemoyer, L., & Stoyanov, V. (2019). RoBERTa: A Robustly Optimized BERT Pretraining Approach. *arXiv* (pp. 1–13). https://doi.org/10.48550/arXiv.1907.11692.
17. Yang, Z., Dai, Z., Yang, Y., Carbonell, J., Salakhutdinov, R., & Le, Q. V. (2019). XLNet: Generalized Autoregressive Pretraining for Language Understanding. In *Proceedings of the 33rd International Conference on Neural Information Processing Systems* (Article 517, pp. 5753–5763).
18. Iosifov, I., Iosifova, O., Romanovskyi, O., Sokolov, V., & Sukailo, I. (2022). Transferability Evaluation of Speech Emotion Recognition between Different Languages. In *Lecture Notes on Data Engineering and Communications Technologies* (pp. 413–426). https://doi.org/10.1007/978-3-031-04812-8_35.
19. K. Khorolska, et al., (2022) Application of a Convolutional Neural Network with a Module of Elementary Graphic Primitive Classifiers in the Problems of Recognition of Drawing Documentation and Transformation of 2D to 3D Models, J. Theor. Appl. Inf. Technol. 100(24) 7426–7437
20. Korshun, N., Myshko, I., & Tkachenko, O. (2023). Automation and Management in Operating Systems: The Role of Artificial Intelligence and Machine Learning. In 20th International Scientific Conference "Dynamical System Modeling and Stability Investigation" (DSMSI), (vol. 3687, pp. 59–68)
21. V. Buhas, et al., (2024) AI-Driven Sentiment Analysis in Social Media Content, in: Workshop on Digital Economy Concepts and Technologies Workshop, DECaT, vol. 3665 12–21
22. Sukaylo, I., & Korshun, N. (2022). THE Influence of NLU and Generative AI on the Development of Cyber Defense Systems. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, *2*(18), 187–196. https://doi.org/10.28925/2663-4023.2022.18.187196
23. D. Shevchuk, et al., (2023) Designing Secured Services for Authentication, Authori-zation, and Accounting of Users, in: Cybersecurity Providing in Information and Telecommunication Systems II Vol. 3550 217–225.