КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (22), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.21.148155
УДК 004.77

Марценюк Максим Станіславович
здобувач освіти спеціальності 125 Кібербезпека
кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID 0000-0002-6662-7610
msmartseniuk.fitm22@kubg.edu.ua

Козачок Валерій Анатолійович
кандидат технічних наук, доцент,
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID 0000-0003-0072-2567
v.kozachok@kubg.edu.ua

Богданов Олександр Михайлович
доктор технічних наук, професор,
професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID 0009-0005-2605-6189
o.bohdanov@kubg.edu.ua

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

Бржевська Зореслава Михайлівна
доктор філософії,
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID 0000-0002-7029-9525
z.brzhevska@kubg.edu.ua

АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ ДЕЗІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ ЗА ДОПОМОГОЮ МАШИННОГО НАВЧАННЯ

Анотація. Соціальні мережі вже давно стали невід'ємною частиною життя сучасного суспільства. Наприклад, в Україні понад 60% населення регулярно використовують їхній функціонал. Для деяких людей сторінки в тій чи іншій соцмережі набули комерційного значення та стали інструментом отримання прибутку. Є й непоодинокі випадки купівлі-продажу акаунтів або порушення авторських прав за допомогою них. Проте наразі в соціальних мережах набирає обертів поширення неточної інформації, спрямованої на введення в оману та завдання серйозної шкоди. Такий процес визначений як «дезінформація». Окрім дезінформації також розрізняють термін «неправдива інформація». Ці терміни не є синонімами, тому їх слід розрізняти для достовірності дослідження. Неправдивою є інформація, що несе неточні дані, які виникли внаслідок помилок, проте цей термін не містить в собі наміру навмисного введення в оману. У свою чергу, термін «дезінформація» навпаки — створений з метою навмисного поширення неправдивої інформації з метою введення в оману інших. В останні роки тема дезінформації, а також її наслідки привернули велику увагу. Незважаючи на те, що дезінформація не є новим явищем, технологічний прогрес створив ідеальну атмосферу для її швидкого поширення. Такі соціальні мережі, як Facebook, Twitter і YouTube, створюють сприятливий ґрунт для створення та поширення дезінформації та неправдивої інформації. Через це постає важливість дослідження, як працюють соціальні медіа, як створюються та поширюються фейкові новини через соціальні медіа

та яку роль відіграють користувачі. Дослідження розглядає соціальні мережі як платформу для поширення дезінформації. Розгляд проблеми взаємодії користувачів із новинами в соціальних мережах доповнює проблематику фейкових новин, розглядаючи проблему взаємодії користувачів із новинами та співпраці в епоху інформації.

Для достовірності дослідження, було розглянуто поняття дезінформації та неправдивої інформації. Наведено вичерпний огляд існуючих підходів до виявлення фейкових новин з точки зору машинного навчання. Алгоритми класифікації на основі машинного навчання відіграють дуже важливу роль у виявленні фейкових новин або чуток у соціальних мережах, що є дуже складним і важким процесом через різноманітні політичні, соціально-економічні та багато інших пов'язаних факторів. У цьому огляді розглядаються різні підходи до машинного навчання, такі як обробка природної мови (NLP), лінійна регресія, метод k-найближчих сусідів (KNN), метод опорних векторів (SVM), довга короткочасна пам'ять (LSTM), штучні нейронні мережі та багато інших.

Ключові слов: соціальна мережа; дезінформація; неправдива інформація; фейкові новини; машинне навчання.

ВСТУП

Соціальною мережею називають веб-сайт або іншу службу в мережі Інтернет, яка дозволяє користувачам створювати публічні або напівпублічні анкети (акаунти), складати списки користувачів, з якими вони мають зв’язок, та переглядати власний список зв’язків і списки інших користувачів [1]. Яскравим прикладом соціальних мереж є Facebook, Instagram, YouTube та ін.

Соціальні мережі вже давно стали невід’ємною частиною життя сучасного суспільства. Наприклад, в Україні понад 60% населення регулярно використовують їхній функціонал [1]. Для деяких людей сторінки в тій чи іншій соцмережі набули комерційного значення та стали інструментом отримання прибутку. Є й непоодинокі випадки купівлі-продажу акаунтів або порушення авторських прав за допомогою них. Проте наразі в соціальних мережах набирає обертів поширення неточної інформації, спрямованої на введення в оману та завдання серйозної шкоди. Такий процес визначений як «дезінформація».

Окрім дезінформації також розрізняють термін «неправдива інформація». Ці терміни не є синонімами, тому їх слід розрізняти для достовірності дослідження. Неправдивою є інформація, що несе неточні дані, які виникли внаслідок помилок, проте цей термін не містить в собі наміру навмисного введення в оману. У свою чергу, термін «дезінформація» навпаки — створений з метою навмисного поширення неправдивої інформації з метою введення в оману інших.

Постановка проблеми. Завдяки Інтернету з’явився новий спосіб поширення новин та інформації в цілому. Раніше люди покладалися на традиційні засоби масової інформації, такі як радіо і телебачення, які включали в себе більше добре відомих джерел новин. Наразі люди все частіше звертаються до онлайн-джерел інформації, таких як соціальні мережі, які дозволяють будь-кому публікувати будь-що без необхідності «перевірки фактів або редакційної оцінки» [2]. Багато людей стурбовані тим, що інтернет-сайти можуть публікувати оманливі матеріали, видаючи їх за «справжні» новини. Дедалі більше людей залучаються до соціальних мереж завдяки зростаючій популярності різноманітних гаджетів з доступом до інтернету та підвищенню швидкості мобільного інтернету. Дійсно, Facebook використовується більшістю людей у всьому світі, і багато хто з нас отримує новини з публікацій у соціальних мережах [3]. Враховуючи нещодавню увагу до ролі соціальних мереж у поширенні фейкових новин

про поточні політичні та соціальні події, дуже важливо зрозуміти, як громадськість взаємодіє з дезінформацією на платформах соціальних мереж. Фейкові новини про сучасні соціальні та політичні проблеми поширюються в соціальних мережах із шаленою швидкістю. Ці містифікації або фейкові історії дезінформують або обманюють аудиторію, як навмисно, так і навпаки. Ці історії зазвичай створюються для того, щоб вплинути на думку людей, просунути політичний порядок денний або заплутати людей, і вони можуть бути прибутковим бізнесом для інтернет-видавців [4]. Такі джерела, як Facebook, Twitter, та інші соціальні медіа-платформи стали важливими ресурсами у наданні новинного контенту. Величезний обсяг інформації та швидкість, з якою вона генерується і поширюється в Інтернеті, робить її практично непідвладною людській перевірці. Тому існує нагальна потреба в розробці технологій, які можуть допомогти людині в автоматичній перевірці фактів і надійному виявленні фейкових новин.

Аналіз останніх досліджень і публікацій. Проведемо аналіз робіт, у яких наведені рішення для виявлення дезінформації.

Автор з командою [5] продемонстрували модель за допомогою методів машинного навчання (ML) та обробки природної мови (NLP), яка збирає статті за допомогою машини опорних векторів (SVM) і вирішує, чи є новина справжньою чи фейковою. Вони використали алгоритм машини опорних векторів для бінарної класифікації для систематизації статей, і на основі цього модель працює, щоб класифікувати статті як справжні або фейкові. У запропонованих моделях вони використовували три основні модулі для уточнення статей або контенту: агрегатор, аутентифікатор і систему пропозицій або рекомендацій. У цій статті вони також використали наївний метод Баєса для перевірки статей на правдивість чи неправдивість і отримали результат з точністю 93,50%, що досягається поєднанням цих трьох алгоритмів, тобто наївний метод Баєса, SVM і NLP.

У звіті Pew Research Center США [6], йдеться про те, що дорослі отримують близько 70% новин із соціальних мереж. З новиною про обрання Дональда Трампа президентом ця інформація призвела до збільшення кількості користувачів Facebook. У цій статті розглядаються лінгвістичні та візуальні особливості, які відіграють свою роль. Таким чином, автори досягли точності близько 83 відсотків.

У роботі [7] автори спостерігали за впливом людей на соціальні медіа і виявили, що 62% дорослих американців залежать від соціальних медіа для отримання новин у 2016 році, що на 13% більше, ніж у 2012 році. Основним джерелом інформації є телебачення. Ми побачили, що ця інформація або безкоштовна, або має дуже низьку вартість, що призводить до появи фейкових новин на цій платформі.

У публікації [8] автори зазначають, що фейкові новини поділяються на клікбейт, впливові та сатиричні. Щоб зупинити фейкові новини, були застосовані такі методи, як виявлення спаму, визначення позиції, набір еталонних даних. Далі автор розглянув аналіз настроїв, який підпадає під методи обробки природної мови. Прикладом фейкових новин, який обговорювався, був «Електорошок» китайського робота з безпеки в аеропорту, що стався в 2016 році і призвів до появи понад 12 тисяч фейкових новин в Китаї, які були розміщені на 244 різних веб-сайтах як джерела.

У [9] автори помітили, що вплив фейкових новин на наше повсякденне життя значно зріс. Вони обговорили 3 підходи для виявлення неправдивих новин: наївний метод Баєса, нейронна мережа, метод опорних векторів. Точність виявлення фейкових новин за допомогою наївного методу Баєса становить 96,08%, тоді як за допомогою двох інших методів, таких як нейронна мережа та метод опорних векторів, точність виявлення фейкових новин становить 99,90%. Автори цієї статті намагаються донести до читачів

інформацію про те, наскільки великий вплив фейкові новини можуть мати на життя людини. Вони обговорюють приклад Таїланду (2017 р.), який зіткнувся з великою катастрофою через поширення фейкових новин про клімат. Автори стверджують, що перед використанням методу машинного навчання вони застосовують метод нормалізації для очищення даних.

У роботі [10] автори досліджували, як виявити фальшиві новини з дописів у Твіттері. Автори, як правило, працюють над постом у Твіттері, тобто над тим, чи є він справжнім, чи фейковим. Вони розповідають про дезінформацію щодо землетрусу в Чилі (2010 р.) та президентських виборів у США. Для виявлення фейкових новин було запропоновано використовувати обробку природної мови. По-перше, вони повинні класифікувати новини, щоб знати, чи є вони справжніми чи фейковими, після чого застосовуються різні типи моделей для отримання результату. Основна увага авторів зосереджена на підвищенні ефективності виявлення фейкових новин, тому вони включили метод довжини слова, який включає підрахунок слів у реченні. Автори використали п’ять різних алгоритмів машинного навчання, а в якості мови програмування використали Python. Серед п’яти методів машинного навчання (ML) — наївний метод Баєса, логістична регресія, метод опорних векторів, рекурентна нейронна мережа та довга короткочасна пам’ять. Автори працюють з текстовими даними, тому вони використали кілька різних ідей для обробки набору даних, а саме: лічильні вектори, TF-IDF, вбудовування слів. Автори також запропонували чотири вектори ознак: вектори підрахунку, вектори на рівні слів, N-грамові вектори, вектори на рівні символів. У результаті, метод опорних векторів (SVM) виявився найкращою моделлю для виявлення фейкових новин.

У роботі [11] автори зазначають, що соціальні медіа є ключовою проблемою сучасного життя. Будь-хто може зареєструватися як видавець новин на соціальних платформах, поширюючи інформацію без перевірки. Це дуже швидко вводить суспільство в оману. Таким чином, автори вважають, що соціальні медіа є платформою для поширення дезінформації. Автори запропонували деякі ознаки для виявлення неправдивих новин — це ознаки, що виділяються з новинної статті, джерела новин та з навколишнього середовища. Для виявлення фейкових новин також використовуються текстові ознаки. Для вилучення тексту з зображень і відео використовується техніка обробки зображень. Загальна кількість текстових ознак, які оцінюються автором, становить 141. Лексичні ознаки, семантичні ознаки, мовні ознаки та психолінгвістичні ознаки згруповані в групи. Автор використав класифікатор для вимірювання сили ознак. Це класифікатор K-найближчих сусідів, наївного методу Баєса, випадкового лісу та методу опорних векторів. Для вимірювання ефективності кожного класифікатора автор використовував площу під ROC-кривою та показник Marco F1 Score. Площа під кривою є більш релевантною для виявлення фейкових новин, тоді як оцінка Macro F1 показує загальну функцію класифікатора.

У роботі [12] авторами розглянуто класифікацію систем штучного інтелекту, моделі штучного інтелекту, які використовуються продуктами безпеки, їх можливості, наведено рекомендації, які слід враховувати під час використання генеративних технологій штучного інтелекту щодо систем кіберзахисту.

Мета статті. Мета статті полягає у аналізі та оцінці результативності існуючих підходів виявлення дезінформації.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Порівняльний аналіз існуючих підходів

У таблиці 1 наведено вичерпний огляд існуючих підходів до виявлення фейкових новин з точки зору машинного навчання. Серед цих підходів деякі класифікатори дали бажаний результат. У статті [9] автори Supanya та ін. досягли найвищого показника точності 99,90%, використовуючи метод опорних векторів, наївний метод Баєса та нейронну мережу. Усі класифікатори, які розглядалися в таблиці, використовували деякі текстові ознаки, N-граму, F-1 Score тощо. Використовуючи ці ознаки, класифікатори працюють краще, і автори намагаються підвищити точність виявлення фейкових новин. Ця таблиця показує, які класифікатори є кращими порівняно з іншими. Отже, серед усіх цих класифікаторів найкращими є метод опорних векторів та наївний метод Баєса, які дають найвищий результат.

Таблиця 1

Огляд існуючих підходів до виявлення фейкових новин з точки зору машинного навчання

Автор	Підхід	Набір даних	Точність
Jain та ін. [5]	наївний метод Баєса, метод опорних векторів та обробка природної мови	Різні новинні сайти, RSS-стрічки	93,5%
Supanya та ін. [9]	метод опорних векторів, нейронна мережа та наївний метод Баєса	Дані були зібрані з 948 373 повідомлень через API Twitter	99,9%
Abdullah-All-Tanvir та ін. [10]	метод опорних векторів, наївний метод Баєса, логістична регресія, довга короткочасна пам’ять та рекурентна нейронна мережа	20 360 даних було зібрано з Чилі, набір даних землетрусу 2010 року	89,34%
Julio CS та ін. [11]	метод k-найближчих сусідів, метод опорних векторів та наївний метод Баєса	Новини від Buzzfeed	89%

Дуже важко дізнатися про факт новин, які поширюються різними сторонами в соціальних мережах, що суперечать одна одній. Такі новини здебільшого пов’язані з політикою. Отже, серед політичних новин дуже складно класифікувати, чи є новина справжньою або фейковою. Для розрізнення таких типів новин на справжні чи фейкові потрібні більш потужні та складні моделі, які можуть легко і дешево класифікувати новини. Ще одним великим викликом у соціальних мережах є перевірка автентичності авторів або видавців новин. У наш час дуже легко створити сторінку у Facebook, Instagram чи будь-якій іншій соціальній мережі, а також канал на Youtube. Тож будь-хто може публікувати новини через ці платформи. Це і створює нову проблематику — знати, хто з авторів є фейковим, а хто справжнім. Ось чому дуже важливо розробити модель, за допомогою якої можна легко перевірити автентичність авторів і видавців новин. Ці моделі допоможуть читачам онлайн-новин вирішувати, новини якого автора варто читати, а якими варто знехтувати.

ВИСНОВКИ

В оглядовому дослідженні обговорюється новаторська робота в галузі виявлення неправдивих новин. Алгоритми класифікації на основі машинного навчання відіграють дуже важливу роль у виявленні фейкових новин або чуток у соціальних мережах, що є дуже складним і важким процесом через різноманітні політичні, соціально-економічні та багато інших пов'язаних факторів. У цьому огляді розглядаються різні підходи до машинного навчання, такі як обробка природної мови (NLP), лінійна регресія, метод k-найближчих сусідів (KNN), метод опорних векторів (SVM), довга короткочасна пам'ять (LSTM), штучні нейронні мережі та багато інших.

У подальшому планується проведення досліджень сучасніших методів виявлення дезінформації в соціальних мережах та розробка рекомендацій щодо її блокування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Прокопенко, В. (2021). *Правова природа сторінок у соціальних мережах*. Юридична газета – онлайн версія. https://yur-gazeta.com/publications/practice/zahist-intelektualnoyi-vlasnosti-avtorske-pravo/pravova-priroda-storinok-u-socialnih-merezhah.html
2. Aldwairi, M., Alwahedi, A. (2018). Detecting Fake News in Social Media Networks. *Procedia Computer Science, 141*, 215–222. https://doi.org/10.1016/j.procs.2018.10.171
3. Stephen, A. (2016). The role of digital and social media marketing in consumer behavior. *Current Opinion in Psychology, 10*, 17–21. https://doi.org/10.1016/j.copsyc.2015.10.016
4. Brennen, B. (2017). Making sense of lies, deceptive propaganda, and fake news. *Journal of Media Ethics, 32(3)*, 179–181.
5. Jain, A., et al. (2019). A smart System for Fake News Detection Using Machine Learning. *2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 1*.
6. Yang, S., et al. (2019). Unsupervised fake news detection on social media: A generative approach. *AAAI Conference on Artificial Intelligence, 33*. https://doi.org/10.1609/aaai.v33i01.33015644
7. Shu, K., et al. (2017). Fake news detection on social media: A data mining perspective. *ACM SIGKDD explorations newsletter, 19(1)*, 22–36. https://doi.org/10.1145/3137597.3137600
8. O'Brien, N. (2018). Machine learning for detection of fake news. Diss. Massachusetts Institute of Technology. https://dspace.mit.edu/handle/1721.1/119727
9. Aphiwongsophon, S., & Chongstitvatana, P. (2018). Detecting fake news with machine learning methods. *2018 15th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications & Information Technology (ECTI-CON)*. https://ieeexplore.ieee.org/document/8620051
10. Abdullah-All-Tanvir, et al. (2019). Detecting Fake News using Machine Learning and Deep Learning Algorithms. *2019 7th International Conference on Smart Computing and Communications (ICSCC)*. https://ieeexplore.ieee.org/document/8843612
11. Reis, J., et al. (2019). Supervised learning for fake news detection. *IEEE Intelligent Systems, 34(2)*, 76–81. https://ieeexplore.ieee.org/document/8709925
12. Сукайло, І., & Коршун, Н. (2022). Вплив NLU і генеративного ШІ на розвиток систем кіберзахисту. *Кібербезпека: освіта, наука, техніка, 2(18)*, 187–196.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (22), 2023
ISSN 2663 - 4023

Martseniuk Maksym
student of the Department of Information and Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID 0000-0002-6662-7610
msmartseniuk.fitm22@kubg.edu.ua

Valerii Kozachok
PhD, associate professor, associate professor of the Department of Information and Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID 0000-0003-0072-2567
v.kozachok@kubg.edu.ua

Oleksandr Bohdanov
Doctor of Science, professor, professor of the Department of Information and Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID 0009-0005-2605-6189
o.bohdanov@kubg.edu.ua

Ievgen Iosifov
PhD. Student of Department of Information and Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID 0000-0001-6203-9945
y.iosifov.asp@kubg.edu.ua

Zoreslava Brzhevska
PhD, associate professor of the Department of Information and Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID 0000-0002-7029-9525
z.brzhevska@kubg.edu.ua

ANALYSIS OF METHODS FOR DETECTING MISINFORMATION IN SOCIAL NETWORKS USING MACHINE LEARNING

Abstract. Social networks have long become an integral part of the life of modern society. For example, in Ukraine, more than 60% of the population regularly use their functionality. For some people, pages in one or another social network have acquired commercial significance and have become a tool for generating income. There are also rare cases of buying and selling accounts or violating copyright with their help. However, the spread of inaccurate information aimed at misleading and causing serious harm is gaining momentum in social networks. Such a process is defined as "disinformation".

In addition to disinformation, the term "false information" is also distinguished. These terms are not synonymous, so they should be distinguished for the validity of the study. Misrepresentation is information that contains inaccurate information resulting from errors, but the term does not include the intent to mislead. In turn, the term "disinformation", on the contrary, is created for the purpose of deliberately spreading false information with the aim of misleading others.

In recent years, the topic of disinformation, as well as its consequences, has attracted a lot of attention. Although disinformation is not a new phenomenon, technological advances have created the perfect environment for its rapid spread. Social networks such as Facebook, Twitter and YouTube create fertile ground for the creation and dissemination of misinformation and false information. This makes it important to research how social media works, how fake news is created and spread through social media, and what role users play.

The study examines social media as a platform for spreading misinformation. Consideration of the problem of user interaction with news in social networks complements the problem of fake news by considering the problem of user interaction with news and collaboration in the information age.

For the reliability of the research, the concepts of misinformation and false information were considered. A comprehensive review of existing approaches to detecting fake news from the point of view of machine learning is given.
Machine learning based classification algorithms play a very important role in detecting fake news or rumors in social media, which is a very complex and difficult process due to various political, socio-economic and many other related factors.
This review covers various machine learning approaches such as Natural Language Processing (NLP), linear regression, k-Nearest Neighbors (KNN), Support Vector Method (SVM), Long Short-Term Memory (LSTM), artificial neural networks and many others.

Keywords: social network; misinformation; false information; fake news; machine learning.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Prokopenko, V. (2021). *Legal nature of pages in social networks*. Legal newspaper - online version. https://yur-gazeta.com/publications/practice/zahist-intelektualnoyi-vlasnosti-avtorske-pravo/pravova-priroda-storinok-u-socialnih-merezhah.html
2. Aldwairi, M., Alwahedi, A. (2018). Detecting Fake News in Social Media Networks. *Procedia Computer Science, 141*, 215–222. https://doi.org/10.1016/j.procs.2018.10.171
3. Stephen, A. (2016). The role of digital and social media marketing in consumer behavior. *Current Opinion in Psychology, 10*, 17–21. https://doi.org/10.1016/j.copsyc.2015.10.016
4. Brennen, B. (2017). Making sense of lies, deceptive propaganda, and fake news. *Journal of Media Ethics, 32(3)*, 179–181.
5. Jain, A., et al. (2019). A smart System for Fake News Detection Using Machine Learning. *2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 1*.
6. Yang, S., et al. (2019). Unsupervised fake news detection on social media: A generative approach. *AAAI Conference on Artificial Intelligence, 33*. https://doi.org/10.1609/aaai.v33i01.33015644
7. Shu, K., et al. (2017). Fake news detection on social media: A data mining perspective. *ACM SIGKDD explorations newsletter, 19(1)*, 22–36. https://doi.org/10.1145/3137597.3137600
8. O'Brien, N. (2018). Machine learning for detection of fake news. Diss. Massachusetts Institute of Technology. https://dspace.mit.edu/handle/1721.1/119727
9. Aphiwongsophon, S., & Chongstitvatana, P. (2018). Detecting fake news with machine learning methods. *2018 15th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications & Information Technology (ECTI-CON)*. https://ieeexplore.ieee.org/document/8620051
10. Abdullah-All-Tanvir, et al. (2019). Detecting Fake News using Machine Learning and Deep Learning Algorithms. *2019 7th International Conference on Smart Computing and Communications (ICSCC)*. https://ieeexplore.ieee.org/document/8843612
11. Reis, J., et al. (2019). Supervised learning for fake news detection. *IEEE Intelligent Systems, 34(2)*, 76–81. https://ieeexplore.ieee.org/document/8709925
12. Sukailo, I., & Korshun, N. (2022). The influence of NLU and generative AI on the development of cyber defense systems. *Cyber security: education, science, technology, 2(18)*, 187–196.