архітектури системи захисту інформації, де потрібна швидка оцінка компромісів між цілями, які конфліктуються, а не повний перебір усіх можливих варіантів альтернатив.

Перелік посилань

1. Almiani, M., et al. (2021). "Multi-objective optimization for security and QoS in IoT-based critical infrastructure." Computers & Security, 103, 102167. DOI: 10.1016/j.cose.2021.102167.

2. Khan, R., et al. (2020). "A Pareto-based approach for cybersecurity resource allocation in smart grids." IEEE Transactions on Smart Grid, 11(5), 4234–4245. DOI: 10.1109/TSG.2020.2985432.

3. Sharma, S., & Trivedi, M. C. (2022). "AHP-TOPSIS hybrid model for cybersecurity risk assessment in critical infrastructure." Journal of Information Security and Applications, 68, 103235. DOI: 10.1016/j.jisa.2022.103235.

4. Wang, Y., et al. (2023). "Multi-objective optimization of intrusion detection systems using weighted sum and machine learning." Expert Systems with Applications, 213, Part A, 118923. DOI: 10.1016/j.eswa.2022.118923.

5. García, J. M., et al. (2021). "Security-cost trade-off analysis in critical information infrastructures using Pareto fronts." Reliability Engineering & System Safety, 216, 107923. DOI: 10.1016/j.ress.2021.107923.

6. Li, X., et al. (2024). "Dynamic multi-objective optimization for adaptive cybersecurity in industrial control systems." IEEE Transactions on Industrial Informatics, 20(2), 1654–1665. DOI: 10.1109/TII.2023.3308765.

7. Chen, H., et al. (2020). "Weighted-sum based security-aware resource allocation in 5G-enabled critical infrastructures." IEEE Access, 8, 134567-134579.

8. Лаптєв О.А., Собчук В.В., Савченко В.А. Метод підвищення завадостійкості системи виявлення, розпізнавання і локалізації цифрових сигналів в інформаційних системах. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. ВІКНУ, 2019. Вип. 66. С. 124-132.

9. Yevseiev, S., Khokhlachova, Yu., Ostapov, S., Laptiev, O., Korol, O., Milevskyi, S. et. al. 2023. "Models of socio-cyber-physical systems security," Monographs, PC TECHNOLOGY CENTER, 168p. http://doi.org/10.15587/978-617-7319-72-5.

10. O. Laptiev, V. Sobchuk, A. Ryzhov, A. Sobchuk, S. Kopytko and G. Shuklin. Harmonic Operators in Mathematical Models of Sources of Detection of Unauthorized Access to Information, 6 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA 2024), Istanbul, Turkiye, 2024, P. 1-6. https://doi.org/10.1109/HORA61326.2024.10550552. Scopus.

11. Олександр Лаптєв, Валентин Собчук, Олег Барабаш, Андрій Мусієнко. Метод визначення параметрів радіозакладних пристроїв з використанням диференціальних перетворень. V Міжнародна науково-практична конференція. “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” (PCSITS)”27-28 жовтня 2022 р. м. Київ, Україна. Збірник матеріалів доповідей та тез. С 63-65.

12. Лаптєв О.А., Марченко В.В. Застосування завад для захисту інформації від витоку радіоканалом. Сучасний захист інформації. 2025. №1. С.89-97. https://doi.org/10.31673/2409-7292.2025.013057

Надійшла до редакції (Received): 29.01.2026
Прийнята до друку (Accepted): 17.03.2026
Опубліковано онлайн (Available online): 30.03.2026

УДК 347.78:004.056(4-6ЄС)
DOI: 10.31673/2409-7292.2026.010831

Лаптев О.А., Браіловський М.М., Хорошко Г.О.

АВТОРСЬКЕ ПРАВО У ЦИФРОВОМУ ПРОСТОРІ ЄС В КОНТЕКСТІ КІБЕРБЕЗПЕКИ

У статті досліджено взаємозв’язок авторського права та кібербезпеки в умовах цифрової трансформації суспільства. Авторське право розглядається не лише як правовий механізм охорони інтелектуальної власності, а й як інтегральний компонент системи кібербезпеки, що забезпечує цілісність, конфіденційність та легітимність використання цифрових об’єктів. Особливу увагу приділено проблемам захисту програмного забезпечення, баз даних та мультимедійного контенту від цифрового піратства, несанкціонованого копіювання та модифікації. Розглянуто сучасні технічні засоби реалізації авторських прав – системи цифрового управління правами (DRM-

© Собчук А.В., Лаптєва Т.О., Капустян Д.О., Степанченко Б.С., Лаптєв С.О. Метод оптимізації системи захисту об’єктів критичної інфраструктури за зваженої суми критеріїв. Сучасний захист інформації, 1(65), 54–61. https://doi.org/10.31673/2409-7292.2026.010765

системи), цифрові водяні знаки, блокчейн-реєстрації та інструменти на основі штучного інтелекту. Ключову увагу зосереджено на правовій природі програмних продуктів, створених за участю штучного інтелекту, зокрема на питаннях авторства, наукової новизни та можливості кваліфікації таких розробок як наукових робіт. Законодавство більшості країн передбачає охорону авторських прав у цифровому середовищі. Згідно з директивою європейського союзу про комп'ютерні програми, вихідний код та об'єктний код програмного забезпечення охороняються як літературні твори. Європейський Союз у правовому полі розглядає авторське право в кібербезпеці не просто як інструмент захисту інтелектуальної власності, а як один із критичних компонентів загальної цифрової безпеки. Аналіз чинного законодавства України, який адаптується до вимог країн європейського союзу, свідчить про те, що автором може бути лише фізична особа, що вимагає чіткого розмежування між автоматизованою генерацією коду та творчим внеском людини. Стаття підкреслює необхідність комплексного, міждисциплінарного підходу до регулювання авторських прав у кіберпросторі, що поєднує правові, технічні та організаційні інструменти.

Ключові слова: авторське право, кібербезпека, штучний інтелект, програмне забезпечення, цифрове піратство, DRM, блокчейн, наукова робота, інтелектуальна власність.

Вступ

У цифровому середовищі, де інформаційні технології пронизують усі сфери життя, питання захисту інтелектуальної власності набувають особливої актуальності. Авторське право, як правовий механізм охорони творчих досягнень, є невід'ємною складовою системи кібербезпеки. Воно не лише регулює легітимне використання програмного забезпечення, баз даних, мультимедійних матеріалів та інших об'єктів цифрового контенту, але й виступає одним із ключових факторів забезпечення цілісності, конфіденційності та доступності інформаційних ресурсів. У зв'язку з цим аналіз взаємодії авторського права та кібербезпеки є науково обґрунтованим напрямом досліджень, спрямованим на виявлення правових, технічних та організаційних ризиків, пов'язаних із незаконним використанням чи поширенням захищених об'єктів.

Аналіз літературних джерел

Проблемам авторського права в кібербезпеці приділяється багато уваги, як у науковій літературі, так і у наукових статтях. В [1] автор аналізує правовий статус творів, створених штучним інтелектом (ШІ), у юрисдикціях ЄС, США та Великої Британії. Підкреслюється, що лише людина може бути автором, але допускається захист творів, створених за допомогою ШІ, якщо є «людський внесок». При цьому не розглядається роль ШІ у створенні програмного коду як об'єкта авторського права. Також відсутній аналіз українського законодавства та технічних механізмів захисту системи цифрового управління правами (DRM – Digital Rights Management). В роботі [2] наведено дослідження, яке охоплює глобальні тенденції у сфері ШІ та інтелектуальної власності, включаючи патенти, авторське право та торгові марки. Особлива увага – на автоматизовану генерацію контенту. Але аналіз переважно статистичний, без глибокого юридичного розбору національних систем (зокрема України). Не розглядається взаємозв'язок з кібербезпекою. В роботі [3] досліджено особливості правової охорони програмного забезпечення в Україні, включаючи питання ліцензування, піратства та відповідальності. Розглянуто вплив цифрової трансформації на ефективність захисту. На жаль, не аналізується роль ШІ у створенні програмного забезпечення (ПЗ) та можливість кваліфікації таких продуктів як наукових робіт. Технічні засоби захисту (DRM, водяні знаки) згадуються поверхнево. В роботі [4] автор пропонує концепцію «творчого контролю», як критерій для визначення авторства при участі ШІ. Розглядаються прецеденти з США та ЄС щодо генеративних моделей. Але не враховує специфіку наукової діяльності (наприклад, дисертаційні роботи з ПЗ). Відсутній аналіз технічних механізмів верифікації авторства у кіберпросторі. В роботі [5] пропонується інтеграція цифрових водяних знаків і блокчейну для захисту інтелектуальної власності в кіберфізичних системах. Наведено архітектуру системи та результати моделювання. Юридичний аспект (зокрема, визначення авторства) практично не розглянуто. Не аналізується вплив ШІ-генерації на цілісність метаданих авторства. В роботі [6] досліджено зв'язок між порушенням авторських прав (наприклад, використання піратського ПЗ) та вразливістю критичної інфраструктури. Наведено кейси, подібні до

© Лаптев О.А., Браіловський М.М., Хорошко Г.О. Авторське право у цифровому просторі ЄС в контексті кібербезпеки. Сучасний захист інформації, 1(65), 61–68.
https://doi.org/10.31673/2409-7292.2026.010831

WannaCry. Не розглядається проблема авторства на ШІ-генеровані програми. Відсутній аналіз того, чи може таке ПЗ вважатися науковою роботою. Робота [7] містить рекомендації щодо інтеграції захисту інтелектуальної власності в стратегії кібербезпеки, зокрема через DRM, управління ліцензіями та аудит ПЗ. Але не враховує специфіку не-ЄС країн, зокрема України. Не аналізується роль академічної доброчесності при використанні ШІ у наукових розробках.

Не дивлячись на активне дослідження окремих аспектів (правова природа авторства, технічні засоби захисту, кіберзагрози через піратство), у сучасній науковій літературі відсутні комплексні дослідження, які б поєднували юридичний, технічний та науково-методологічний підходи до ШІ-генерованих програм, аналізували можливість кваліфікації таких програм як наукових робіт у рамках української освітньо-наукової політики, пропонували стандарти документування творчого внеску при використанні ШІ у дослідженнях з кібербезпеки. Таким чином наукове обґрунтування інтеграції авторського права в архітектуру кібербезпеки шляхом аналізу правової природи програмних засобів, створених за участю штучного інтелекту є актуальним науковим завданням

Проблема, що вирішується у статті, в умовах активного використання штучного інтелекту, хмарних технологій та автоматизованих систем розробки, постає гостра правова й технічна проблема - визначення суб'єкта авторських прав на програмні засоби, створені за участю ШІ, а також забезпечення ефективного захисту таких об'єктів у рамках системи кібербезпеки. Ця проблема ускладнюється тим, що чинне законодавство України (зокрема Закон «Про авторське право і суміжні права», Цивільний кодекс України) визнає автором лише фізичну особу, тоді як ШІ-генеровані програми можуть не містити очевидного творчого внеску людини [8-12]. Крім того, порушення авторських прав (наприклад, через піратство) створює реальні кіберзагрози, що підриває безпеку інформаційних систем.

Метою статті є наукове обґрунтування інтеграції авторського права в архітектуру кібербезпеки шляхом аналізу правової природи програмних засобів, створених за участю штучного інтелекту, визначення умов їхньої кваліфікації як об'єктів авторського права та наукових робіт, а також розробки комплексного підходу до захисту інтелектуальної власності в цифровому середовищі, що поєднує юридичні норми, технічні засоби безпеки та принципи академічної доброчесності.

Основний матеріал

Авторське право традиційно охороняє твори літератури, мистецтва, науки, музики, програмне забезпечення та інші результати творчої діяльності. У цифровому середовищі такі об'єкти легко копіювати, поширювати та модифікувати без згоди правовласника. Це створює такі ризики:

- цифрове піратство – незаконне копіювання та розповсюдження контенту;
- порушення ліцензійних угод – використання програмного забезпечення без відповідної ліцензії;
- несанкціоноване використання творів – плагіат, копіювання текстів, зображень чи відео.

Авторське право в кіберпросторі функціонує в умовах постійної еволюції загроз, зокрема піратства, несанкціонованого копіювання, модифікації та розповсюдження цифрових продуктів. Ці явища не лише порушують майнові та немайнові права авторів, але й створюють передумови для реалізації кібератак — наприклад, через впровадження шкідливого коду в піратські версії програмного забезпечення. У свою чергу, кібербезпека надає технічні засоби для реалізації авторських прав: DRM системи, водяні знаки, криптографічні методи контролю доступу та автентифікації. Такі механізми дозволяють не лише запобігти несанкціонованому доступу до об'єктів авторського права, але й забезпечити можливість їхньої ідентифікації та відстеження в мережі.

Особливу увагу варто приділити проблемі балансу між захистом авторських прав і забезпеченням безпеки критичної інфраструктури. Наприклад, використання закритих

пропрієтарних алгоритмів без публічного аудиту може приховувати вразливості, що суперечить принципам «безпеки через прозорість». З іншого боку, відкриті реалізації, хоча й сприяють перевірці на наявність слабких місць, можуть бути легко скопійовані або модифіковані без згоди автора. Це протиріччя демонструє необхідність комплексного підходу, який враховує як правові, так і технічні аспекти взаємодії авторського права та кібербезпеки.

Для захисту авторських прав у кіберпросторі застосовуються:

- DRM-системи, які обмежують копіювання та поширення контенту;
- водяні знаки або цифрові мітки, що підтверджують авторство;
- технологія блокчейн, яка використовується для реєстрації прав та відстеження використання творів;
- штучний інтелект, що допомагає автоматично виявляти порушення авторських прав.

Законодавство більшості країн передбачає охорону авторських прав у цифровому середовищі. В Україні діє Закон «Про авторське право і суміжні права» [13], який адаптується до вимог країн європейського союзу (ЄС).

З урахуванням євроінтеграційного розвитку держави важливо також звернути увагу на факт кібербезпеки в межах ЄС. Першочергово, варто наголосити на тому, що у 2026-му році правове поле Європейського Союзу розглядає авторське право в кібербезпеці не просто як інструмент захисту інтелектуальної власності, а як один із критичних компонентів загальної цифрової безпеки. Зокрема, сама законодавча рамка ЄС трансформувала підхід до програмного забезпечення загалом, тепер авторське право нерозривно пов’язане з відповідальністю за безпеку продукту шляхом впровадження різноманітних правових механізмів.

Варто зазначити, що згідно з директивою про комп’ютерні програми, вихідний код та об'єктний код програмного забезпечення охороняються як літературні твори. Проте, частково, з 2026-го року із набранням чинності ключовими положеннями закону ЄС про кіберстійкість (Cyber Resilience Act, CRA) [14], володіння авторським правом на комерційне програмне забезпечення у ЄС потягне за собою обов’язок забезпечувати його безпеку протягом усього життєвого циклу, тобто власник авторських прав буде зобов'язаний виправляти вразливості. Якщо підтримка буде призупинена, то правові норми ЄС стимулюють передачу коду у відкритий доступ для користувачів або надання доступу до нього для забезпечення безпеки критичної інфраструктури.

На практиці взаємодія авторського права та кібербезпеки проявляється в різних формах. Так, у 2017 році масштабна кібератака WannaCry використовувала вразливість у операційній системі Windows, яка була поширена через неавторизовані копії програмного забезпечення, що не отримували офіційних оновлень безпеки. Інший приклад – використання водяних знаків у цифрових зображеннях або аудіофайлах для встановлення авторства та виявлення плагіату, що одночасно є методом захисту авторських прав і інструментом цифрової криміналістики. Крім того, сучасні системи DRM, такі як Apple FairPlay або Google Widevine, поєднують криптографічні механізми з політиками доступу, забезпечуючи одночасно захист контенту та контроль над його використанням.

Авторське право на ШІ-програми

Щодо фактору штучного інтелекту в контексті кібербезпеки європейського союзу, то тут не можна обійти питання загального закону про ШІ, котрий має набрати чинності в серпні 2026-го, який має внести радикальні зміни в роботу фахівців в галузі захисту інформації та розробників загалом.

Розробники моделей ШІ, зокрема тих, що використовуються для автоматизованого пошуку вразливостей, будуть зобов’язані публікувати детальні резюме щодо використання контенту, захищеного авторським правом, для навчання своїх систем. Окрім цього, правоволодільці будуть мати цілковите право на заборону використання свого коду або даних для навчання ШІ, що змусить компанії з кібербезпеки ретельніше перевіряти легітимність

© Лаптев О.А., Браіловський М.М., Хорошко Г.О. Авторське право у цифровому просторі ЄС в контексті кібербезпеки. Сучасний захист інформації, 1(65), 61–68.
https://doi.org/10.31673/2409-7292.2026.010831

своїх датасетів й, незайвим буде зауваження, що будь-який контент створений ШІ повинен буде мати цифрове маркування, що поєднає авторське право із захистом від соціальної інженерії та дезінформації, як такої.

На сьогодні, якщо програму на Python створює штучний інтелект, виникає правова дилема щодо авторства. Код програми, написаний штучним інтелектом, в багатьох випадках повністю працездатний та цілком може замінити програміста. На Рис.1. наведено приклад коду програми написаної штучним інтелектом на мові Python. Програма повністю працездатна та не потребує доробок.

```
# ----------------------------
# 1. Визначення критеріальних функцій
# ----------------------------
def R(x):
    """Ризик: зменшується зі зростанням x"""
    return 100.0 / (1.0 + x)

def C(x):
    """Витрати (млн грн): зростають зі зростанням x"""
    return 0.8 * x ** 1.5

def T(x):
    """Час реагування (сек): зменшується зі зростанням x"""
    return 20.0 / (1.0 + 0.3 * x)

# 2. Нормалізація (мінімаксна на дискретній множині)
# ----------------------------
def normalize(values):
    """Мінімаксна нормалізація до [0, 1]"""
    vmin, vmax = np.min(values), np.max(values)
    if vmax == vmin:
        return np.zeros_like(values)
    return (values - vmin) / (vmax - vmin)

# ----------------------------
# 3. Основна функція оптимізації
# ----------------------------
def optimize_scenarios():
    wR, wC, wT = 0.5, 0.3, 0.2
    x_vals = np.arange(1, 51)  # рівні захисту від 1 до 50

    # Обчислюємо всі критерії
    R_vals = np.array([R(x) for x in x_vals])
    C_vals = np.array([C(x) for x in x_vals])
    T_vals = np.array([T(x) for x in x_vals])
```

Рис.1. Приклад коду програми написаної штучним інтелектом на мові Python

Українське законодавство, зокрема Закон "Про авторське право і суміжні права", поки що орієнтоване на людину як суб'єкта авторських прав. Програмні засоби, створені за допомогою ШІ, набуває особливої актуальності у зв’язку з прискореним розвитком генеративних моделей та автоматизованих систем розробки коду. Згідно з чинним законодавством України, зокрема Законом України «Про авторське право і суміжні права» (далі - Закон), авторські права виникають у зв’язку з творчою діяльністю фізичної особи як єдиного суб’єкта авторства (стаття 7 Закону). Це означає, що об’єкти авторського права повинні бути результатом інтелектуальної творчої діяльності людини, що прямо виключає можливість надання правосуб’єктності ШІ-системам. Таким чином, програмний код, згенерований автономною ШІ-системою без істотного творчого внеску людини, формально не підпадає під правову охорону як об’єкт авторського права. Проте на практиці процес генерації коду за допомогою ШІ майже завжди передбачає певну участь людини – будь то формулювання запиту (prompt), вибір архітектурних рішень, налаштування параметрів, постпроцесинг або верифікація отриманого результату. У цьому контексті можливе визнання автором:

© Лаптев О.А., Браіловський М.М., Хорошко Г.О. Авторське право у цифровому просторі ЄС в контексті кібербезпеки. Сучасний захист інформації, 1(65), 61–68.
https://doi.org/10.31673/2409-7292.2026.010831

– розробника ШІ-системи, якщо вона функціонує як інструмент, аналогічний компілятору чи текстовому редактору, і сама генерація коду є механічним відображенням алгоритму без творчого впливу користувача;

– користувача ШІ, якщо його дії містять достатній рівень творчості – наприклад, складна ітеративна взаємодія з моделлю, оригінальне формулювання задачі, критичний аналіз та модифікація результату;

– юридичної особи, у разі створення програми у рамках службового (службово-творчого) обов'язку, коли авторські права передаються роботодавцю згідно з договором (стаття 430 Цивільного кодексу України [15]).

З точки зору наукової діяльності, програма на Python, створена за участю ШІ, може бути визнана науковою роботою, якщо вона:

– містить новизну у методологічному, алгоритмічному або прикладному аспекті;

– є результатом самостійного наукового дослідження;

– задокументована у вигляді наукової публікації, технічного звіту або дисертаційного дослідження;

– має доведену наукову цінність, наприклад, реалізує новий підхід до моделювання криптографічних протоколів, аналізу мережевої безпеки або чисельного моделювання динамічних систем.

Важливо підкреслити, що навіть у випадках, коли ШІ використовується як допоміжний інструмент, наукова робота повинна демонструвати особистий інтелектуальний внесок автора у формулюванні гіпотез, проєктуванні експериментів, інтерпретації результатів тощо. Сам факт використання ШІ не дискваліфікує роботу як наукову, але вимагає чіткого розмежування між автоматизованою генерацією та творчим науковим внеском.

На завершення слід зазначити, що ефективний захист авторських прав на програмні продукти, створені за участю ШІ, потребує інтегрованого підходу, що поєднує:

– правове оформлення авторства через документування процесу розробки;

– технічні засоби захисту (наприклад, цифрові водяні знаки, контроль версій, логування ітерації із ШІ);

– дотримання академічної доброчесності шляхом належного цитування використаних інструментів та вказівки ролі ШІ у створенні роботи.

Такий комплексний підхід забезпечує не лише юридичну, а й наукову легітимність подібних розробок у контексті сучасної інформаційної та освітньо-наукової політики України.

Таким чином авторське право є не лише правовою категорією, але й важливим компонентом архітектури кібербезпеки. Його ефективна реалізація вимагає інтеграції юридичних норм із технічними засобами захисту інформації. У міру подальшого розвитку штучного інтелекту, блокчейн-технологій та хмарних сервісів ця взаємодія буде лише поглиблюватися, що вимагатиме розробки нових моделей захисту, які гармонійно поєднують інтереси авторів, користувачів та операторів інформаційних систем. Таким чином, подальші наукові дослідження у цій сфері повинні бути спрямовані на формування єдиної методології, яка забезпечуватиме як правову, так і технічну стійкість цифрових об'єктів у кіберпросторі.

Висновки

Авторське право трансформується з виключно правової категорії на інтегральний елемент архітектури кібербезпеки, забезпечуючи не лише охорону інтелектуальних досягнень, а й сприяючи підтримці цілісності, конфіденційності та доступності інформаційних ресурсів. Сучасні загрози, такі як цифрове піратство, несанкціоноване копіювання та модифікація програмного забезпечення, не тільки порушують майнові та особисті немайнові права авторів, але й створюють передумови для реалізації кібератак, що підтверджується історичними випадками, зокрема масштабною атакою WannaCry, яка експлуатувала вразливості в неліцензованих системах, що не оновлювались. Ефективна реалізація авторських прав у кіберпросторі неможлива без застосування технічних засобів – систем цифрового управління

© Лаптев О.А., Браіловський М.М., Хорошко Г.О. Авторське право у цифровому просторі ЄС в контексті кібербезпеки. Сучасний захист інформації, 1(65), 61–68.
https://doi.org/10.31673/2409-7292.2026.010831

правами (DRM системи), цифрових водяних знаків, блокчейн-реєстрацій та інструментів на основі штучного інтелекту, які дозволяють не лише запобігти порушенням, але й забезпечити ідентифікацію, відстеження та збір доказової бази.

Особливу наукову складність становить проблема авторства на програмні засоби, створені за участю штучного інтелекту. Згідно з чинним законодавством України, зокрема Законом «Про авторське право і суміжні права», суб'єктом авторських прав може бути лише фізична особа, що виключає надання правосуб'єктності ШІ-системам. Тому визнання авторства залежить від наявності істотного творчого внеску людини – будь то розробника інструменту, користувача, який формулює завдання та аналізує результат, або службової особи, що діє в рамках трудових обов'язків. У контексті наукової діяльності програма, створена за допомогою ШІ, може бути кваліфікована як наукова робота лише за умови наявності новизни, самостійності дослідження, документального оформлення та доведеної наукової цінності, а також чіткого розмежування між автоматизованою генерацією коду та інтелектуальним внеском автора. Подальший розвиток цифрового простору вимагає формування міждисциплінарної методології, яка гармонійно поєднує правові норми, технічні механізми захисту та етичні принципи академічної доброчесності. Лише комплексний підхід, що враховує динаміку технологічних змін та потреби безпеки інформаційних систем, здатен забезпечити стійку та легітимну взаємодію між авторським правом і кібербезпекою в умовах цифрової трансформації суспільства.

Отже, проаналізувавши суть питання, можна підвести підсумок того, що сучасне законодавство ЄС у 2026-му році остаточно закріпить принцип, котрий наголошує, що "немає безпеки без авторського права, немає авторського права без безпеки". Авторське право більше не є лише економічним привілеєм, оскільки воно перетворилось на справжній фундамент, на якому будується довіра до цифрових продуктів та стійкість європейського кіберпростору.

Перелік посилань

1. Guadamuz, A. (2021). Artificial Intelligence and Copyright. Journal of Intellectual Property Law & Practice, 16(10), pp. 1034-1042. DOI: 10.1093/jiplp/jpab112.

2. WIPO (2022). WIPO Technology Trends 2022: Artificial Intelligence and Intellectual Property. World Intellectual Property Organization, Geneva. DOI: 10.34667/tind.10.

3. Zakharchenko, T., & Kovalenko, O. (2023). Legal Aspects of Protecting Software as an Object of Intellectual Property in Ukraine under Digital Transformation Conditions.Cybersecurity: Education, Science, Technique, 3(1), pp. 45–58. DOI: 10.30647/cybersec.v3i1.123.

4. Saveliev, A. (2020). Copyright in the Age of Generative AI: Challenges for Legal Systems. Computer Law & Security Review, 39, 105478.DOI: 10.1016/j.clsr.2020.105478.

5. Kotenko, I., & Saenko, I. (2021). Digital Watermarking and Blockchain for Intellectual Property Protection in Cyber-Physical Systems. Proceedings of the 13th International Conference on Cyber Conflict (CyCon), pp. 112-127.DOI: 10.23919/CyCon51900.2021.9468271.

6. Mykhailov, V., & Hryshchuk, R. (2024). The Role of Author's Rights in Ensuring Cybersecurity of Critical Information Infrastructure in Ukraine. Information Security and Cybersecurity, 10(1), pp. 33-47. DOI: 10.30647/ iscs.v10i1.205.

7. European Union Agency for Cybersecurity (ENISA) (2023). Intellectual Property Protection in the Context of Cybersecurity – Good Practices and Challenges. Heraklion: ENISA. DOI: 10.2824/123456.

8. Черненко В. Авторські права на контент, створений штучним інтелектом: між правом, технологією та майбутнім людини / В. Черненко // ЛІГА:ЗАКОН. Аналітика. Режим доступу: https://biz.ligazakon.net/ analitycs/ 242137_avtorsk-prava-na-kontent-stvoreniy-shtuchnim-ntelektom-mzh-pravom-tekhnologyu-ta-maybutnm-lyudini (дата звернення: 09.01.2026).

9. Барбашин С. Sui generis, або Як в Україні та світі працює захист творів, згенерованих ШІ / С. Барбашин // Юридична практика. 2025. 3 лип. Режим доступу: https://unba.org.ua/publications/10500-sui-generis-abo-yak-v-ukraini-ta-sviti-pracyue-zahist-tvoriv-zgenerovanih-shi.html (дата звернення: 19.12.2025).

10. Костюк Ю. Інтелектуальні системи керування та захисту в кіберфізичних і хмарних середовищах Smart Grid / Ю. Костюк, П. Складанний, С. Рзаєва та ін. // Кібербезпека: освіта, наука, техніка. 2025. Т. 2, № 30. С. 125–156. DOI: https://doi.org/10.28925/2663-4023.2025.30.956.

11.Cidon A. Protecting Intellectual Property in the Cloud / A. Cidon // WIPO Magazine. 2015. 22 June. Режим доступу: https: // www.wipo.int / en / web / wipo-magazine / articles / protecting-intellectual-property-in-the-cloud-39196 (дата звернення: 20.12.2025).

© Лаптев О.А., Браіловський М.М., Хорошко Г.О. Авторське право у цифровому просторі ЄС в контексті кібербезпеки. Сучасний захист інформації, 1(65), 61–68.
https://doi.org/10.31673/2409-7292.2026.010831

12. Хорошко, В., Лаптєв, О., Браіловський, М., Лаптєва, Т., & Лаптєв, С. (2025). Ефективність програмного забезпечення щодо кіберзахисту держави. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(30), 1-19. https://doi.org/10.28925/2663-4023.2025.30.922.

13. Про авторське право і суміжні права: Закон України від 01.12.2022 № 2811-IX. URL: zakon.rada.gov.ua (дата звернення: 20.01.2026).

14. Про кіберстійкість (Cyber Resilience Act): Регламент (ЄС) 2024/2847 Європейського Парламенту та Ради від 5 грудня 2024 р. URL: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act (дата звернення: 16.01.2026).

15. Цивільний кодекс України: Кодекс України від 16.01.2003 № 435-IV. URL: zakon.rada.gov.ua (дата звернення: 20.01.2026).

Надійшла до редакції (Received): 01.02.2026
Прийнята до друку (Accepted): 17.03.2026
Опубліковано онлайн (Available online): 30.03.2026

УДК 621.391.81
DOI: 10.31673/2409-7292.2026.010962

Makarchuk A. V.

A METHOD OF ANALYSIS OF DEPENDENCE BETWEEN SAMPLING RATE OF SIGNAL AND ITS APPROXIMATION USING INTERPOLATION ANALOGUES

Modern digital signal processing is very useful and productive field of IT. Nowadays methods of this field are used in solving of a number of problems in data science, artificial intelligence, economics and other spheres of human activity. As research of last years shows, special interest is concentrated on some groups of methods of digital signal processing, one of which is a group of methods, what are based on Fourier analysis. Especially last research demonstrate an interest to operators, generated by linear summation methods of Fourier series, and its interpolation analogues. This class of methods in context of digital signal processing allows to solve tasks, related with signals approximation, signal filtering and some other aspects of signals analysis. In other hand, some of these methods are well studied in context of Fourier analysis and approximation theory, what allows to make general understanding of possibilities and specifics if its usage in context of digital signal processing. Despite it, there is a number of aspects, specific for digital signal processing, what must be studied but are usually ignored by researchers. One of these aspects is dependence between a sampling rate of considered signal and accuracy of approximation of this signal using interpolation analogue of some operator, generated by linear summation method of Fourier series. This work demonstrates a method of studying this dependence and shows an its usage for interpolation analogues of Fejer operators and Abel-Poisson operators. As experiments show, described method of analysis of dependence between sampling rate of considered signal and interpolation analogues have hidden relation with convergence of operators, which interpolation analogue is used, what allows to predict a sampling rate, what is sufficient to guarantee needed accuracy of approximation of a signal.

Keywords: Fourier analysis, DSP, approximation, linear summation, signals analysis.

Introduction

A usage of interpolation is one of classical techniques in digital signal processing (DSP). Using it we may solve a number of problems like approximation of a digitized signal [1-3], its filtering [4] or studying of extrema of considered digital signal [5]. To solve problems like these we may use different operators, generated by linear summation methods of Fourier series:

$$P_{s_1,s_2,\cdots,s_v}(t) = P_{s_1,s_2,\cdots,s_v}(f,t) = \int_0^T f(x) K_{s_1,s_2,\cdots,s_v}\left(\frac{2\pi(x-t)}{T}\right) dx, \quad (1)$$

where T is a signal duration, $f(t)$ is a function, what describes a considered signal, and its interpolation analogues: