УДК 004.77:004.056.5(477)

ЕТИЧНІ РИЗИКИ ВИКОРИСТАННЯ TILDA ТА ВИБІР БЕЗПЕЧНИХ АЛЬТЕРНАТИВ

С. С. Галун, С. П. Васюта

Національний університет «Львівська політехніка», вул. С. Бандери, 12, Львів, 79013, Україна

У статті комплексно досліджено етичні, безпекові та технологічні ризики використання вебплатформ із країни-агресора, зокрема Tilda Publishing, у контексті сучасної української веброзробки. Проаналізовано особливості правового статусу, зберігання даних, політик конфіденційності та юрисдикційної залежності сервісу, що створює потенційні загрози витоку інформації й непрямого фінансування цифрової інфраструктури держави-агресора. Розглянуто міжнародні стандарти цифрової етики (UNESCO, 2021) та концепції цифрового суверенітету (Roberts, 2024; Floridi, 2022), які визначають необхідність етичного підходу до вибору вебтехнологій.

Дослідження базується на методах контент-аналізу, порівняльного аналізу та етичної оцінки технологій. Проведено огляд наукових публікацій, присвячених питанням відповідального цифрового дизайну, прозорості та підзвітності IT-сервісів. Особливу увагу приділено порівнянню Tilda з альтернативними рішеннями Webflow, WordPress і Carrd за критеріями безпеки, відкритості коду, контролю над даними та відповідності міжнародним етичним нормам. Результати доводять, що використання платформ, пов'язаних із російською юрисдикцією, є несумісним із принципами цифрової етики та національної безпеки України. Натомість етично нейтральні альтернативи, такі як WordPress чи Webflow, забезпечують прозорість, цифрову незалежність і сприяють формуванню культури етичного веброзроблення як складової національної інформаційної стійкості.

Ключові слова: *вебплатформи, цифрова етика, Tilda, Webflow, WordPress, інформаційна безпека, цифровий суверенітет, етична розробка.*

Постановка проблеми. Розвиток no-code платформ істотно спростив створення сайтів, проте їх використання породжує нові ризики — правові, безпекові й етичні [1, с. 4]. У час гібридної війни питання цифрового суверенітету стає ключовим. Українські розробники продовжують використовувати сервіси, пов'язані з країною-агресором, зокрема Tilda, що створює загрози витоку даних і фінансування ворожої інфраструктури [4].

Мета статті. Проаналізувати ризики використання вебплатформ із країни-агресора та обґрунтувати вибір безпечних і етично нейтральних альтернатив для сучасної веброзробки в Україні.

Аналіз публікацій. Аналіз сучасних наукових і публіцистичних джерел засвідчує, що тема етичної відповідальності у веброзробці та питання цифрового суверенітету дедалі частіше розглядаються в контексті національної безпеки та прав людини. У роботі L. Floridi (2022) наголошується, що цифрова етика має розглядатися як моральна основа інфраструктур цифрової держави, а вибір технологій є формою суспільного договору між розробником і користувачем [3]. Дослідник підкреслює, що будь-яке рішення, пов'язане з іноземними сервісами, потребує оцінки з точки зору «етичного коду» — системи цінностей, що лежать в основі технологічної екосистеми.

Згідно з підходом Roberts (2024), цифровий суверенітет має нормативний характер, тобто передбачає етичну відповідальність держави за використання технологій, які не суперечать її політичним і моральним принципам [6, с. 10–12]. Учений розглядає технологічну незалежність як одну з ключових форм прояву суверенітету у XXI столітті, адже залежність від сервісів із юрисдикції держав-агресорів призводить до ослаблення безпекових механізмів і підриває довіру громадян до цифрової держави.

У свою чергу, Fratini (2024) у своєму дослідженні цифрового врядування зазначає, що прозорість і відкритість коду є ключовими ознаками етичного проєктування. Автор доводить, що моделі типу SaaS, які не передбачають локального контролю над даними, створюють ризики порушення прав користувача, особливо у країнах із нестабільним політичним середовищем [7].

Ці підходи перегукуються з висновками Chakraborty, Gupta і Roy (2023), які у своїй статті «Digital Sovereignty and Ethical Design in Web Development» акцентують, що залежність від закритих хмарних платформ без відкритого коду веде до втрати цифрової автономії, а отже — до зниження рівня кіберстійкості держави [8]. Автори наголошують, що держави, які перебувають у зоні конфлікту або санкційного тиску, мають формувати власні незалежні технологічні екосистеми.

У національному дискурсі це питання піднімається у публікаціях Dev.ua (2023), де проаналізовано походження Tilda Publishing та окреслено її зв'язок із російським капіталом і платіжною інфраструктурою [1]. Цей матеріал доповнює наукові підходи практичними доказами того, що використання таких сервісів несе потенційну загрозу інформаційній безпеці та суперечить державній політиці України в умовах війни.

Важливий теоретичний контекст також формують документи міжнародних організацій, зокрема Рекомендація ЮНЕСКО з етики штучного інтелекту (2021), де визначено принципи прозорості, підзвітності та захисту даних як універсальні етичні стандарти для цифрових технологій [2]. Вони прямо співвідносяться з проблематикою вибору вебплатформ, адже кожен сервіс — це не лише інструмент розробки, а й носій певної етичної парадигми.

Таким чином, проведений аналіз свідчить, що попередні дослідження формують цілісну концептуальну основу для розуміння цифрової етики як складової національної безпеки. Науковці одностайно підкреслюють, що використання вебплатформ із юрисдикції країни-агресора не лише несе технічні ризики, а й створює

моральний конфлікт, оскільки суперечить принципам цифрової відповідальності та етичного врядування.

Виклад основного матеріалу. Проведене дослідження базується на поєднанні контент-аналізу, порівняльного підходу та оцінки етичних ризиків використання вебплатформ у сучасній веброзробці. Основну увагу зосереджено на платформі Tilda Publishing, яка виникла у 2014 році в Російській Федерації й активно використовується українськими розробниками для створення корпоративних та інформаційних сайтів.

Попри декларації про міжнародний статус, низка ознак (юридична адреса, платіжна інфраструктура, доменне середовище) свідчить про збереження її часткової залежності від російської юрисдикції. Це створює безпосередні загрози інформаційній безпеці, оскільки будь-який цифровий сервіс, що функціонує під контролем держави-агресора, потенційно може бути використаний для збору даних чи економічного впливу [1; 3].

У ході дослідження встановлено, що Tilda реалізує модель SaaS (Software-as-a-Service), яка не надає користувачу повного контролю над збереженням, резервуванням і передачею даних. Уся серверна інфраструктура перебуває поза юрисдикційним полем українського законодавства, що робить неможливим застосування механізмів правового захисту у випадку порушення конфіденційності або блокування доступу до ресурсу. У роботах Chakraborty, Gupta і Roy (2023) доведено, що SaaS-моделі без відкритого коду підвищують ризики втрати цифрового суверенітету, особливо в країнах із воєнним чи санкційним контекстом [8].

У свою чергу, платформи Webflow та WordPress пропонують різні моделі контролю: перша – повністю хмарна, але з високими стандартами прозорості та чіткою юридичною структурою; друга – децентралізована, що дозволяє повне володіння контентом і базами даних. Саме WordPress (self-hosted) розглядається як приклад «етично нейтральної» технології, що відповідає концепції digital sovereignty – тобто права держав і громад контролювати власну цифрову інфраструктуру [6, с. 9].

Як зазначає Roberts (2024), нормативний цифровий суверенітет має не лише політичний, а й моральний вимір: технологічні рішення повинні бути підзвітними суспільству та не порушувати етичних принципів відповідальності [6, с. 12]. У цьому контексті вибір платформи для веброзробки стає проявом громадянської позиції – рішенням, що визначає, чи підсилює користувач власну державу, чи опосередковано підтримує країну-агресора.

Окремої уваги заслуговує питання прозорості цифрової архітектури. У межах дослідження проведено огляд політик конфіденційності та користувацьких угод Tilda, Webflow і WordPress. Результати свідчать, що лише останні дві чітко регламентують порядок обробки персональних даних відповідно до європейського GDPR (General Data Protection Regulation). У випадку Tilda частина формулювань є розмитими, а вказівки на територію обробки даних не містять конкретних географічних обмежень. Це суперечить рекомендаціям ЮНЕСКО (2021) щодо прозорості й етичного управління інформаційними системами [2].

Додатковим ризиком для українських користувачів є непряма фінансова участь у підтримці цифрової економіки країни-агресора. Оплата преміум-планів Tilda через міжнародні платіжні шлюзи конвертується у прибутки компанії з російським корінням, що становить етичний конфлікт інтересів у період війни. Водночас вибір альтернативних платформ (Webflow, WordPress) не лише усуває ці ризики, а й сприяє розвитку локального IT-середовища завдяки залученню українського хостингу та розробників.

З огляду на результати порівняльного аналізу, можна стверджувати, що використання платформ, пов'язаних із російським капіталом або юрисдикцією, несумісне з принципами цифрової етики. Такі сервіси обмежують технологічний суверенітет, підвищують імовірність втрати даних і суперечать стратегічним інтересам держави.

Натомість перехід на відкриті, етично нейтральні технології відповідає рекомендаціям світових організацій (UNESCO, 2021; Taddeo & Floridi, 2021) і формує передумови для сталого розвитку українського цифрового простору. Це не лише технічний вибір, а й свідомий етичний акт – крок у напрямку утвердження інформаційної незалежності держави.

Висновки. Платформи, пов'язані з РФ, становлять етичну та безпекову загрозу для українських користувачів [3, с. 6]. Перехід на етично нейтральні рішення (Webflow, WordPress) відповідає принципам цифрової етики [6, 7]. Українська спільнота веброзробників має формувати культуру етичного вебпроєктування як складову цифрової безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Dev.ua. Tilda: хто стоїть за популярною платформою. Київ, 2023.
2. UNESCO. Recommendation on the Ethics of Artificial Intelligence. Paris: UNESCO, 2021.
3. Floridi L. et al. The Fight for Digital Sovereignty. Springer, 2022.
4. W3Techs. Content Management System usage statistics. 2024. URL: https://w3techs.com.
5. WordPress Foundation. About the WordPress Project. 2023. URL: https://wordpress.org.
6. Roberts A. Digital Sovereignty and Artificial Intelligence. Springer, 2024.
7. Fratini M. Digital Sovereignty: A Descriptive Analysis and a Critical Review. SSRN, 2024.
8. Chakraborty S., Gupta V., Roy P. Digital Sovereignty and Ethical Design in Web Development. Journal of Cyber Policy, 2023.

REFERENCES

1. Dev.ua. (2023). Tilda: Who stands behind the popular platform. Kyiv.
2. UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence. Paris: UNESCO.
3. Floridi, L., et al. (2022). The Fight for Digital Sovereignty. Springer.
4. W3Techs. (2024). Content Management System usage statistics. Retrieved from https://w3techs.com.
5. WordPress Foundation. (2023). About the WordPress Project. Retrieved from https://wordpress.org.
6. Roberts, A. (2024). Digital Sovereignty and Artificial Intelligence. Springer.

7. Fratini, M. (2024). Digital Sovereignty: A Descriptive Analysis and a Critical Review. SSRN.
8. Chakraborty, S., Gupta, V., & Roy, P. (2023). Digital Sovereignty and Ethical Design in Web Development. Journal of Cyber Policy.

doi: 10.32403/0554-4866-2025-2-90-274-278

ETHICAL RISKS OF USING TILDA AND THE CHOICE OF SAFE ALTERNATIVES

S. S. Halun, S. P. Vasiuta

Lviv Polytechnic National University,
12 S. Bandera Street, Lviv, 79013, Ukraine
serhiy.halun@gmail.com

The article explores the ethical, security, and technological risks of using web platforms originating from the aggressor state, particularly Tilda Publishing, within the framework of modern Ukrainian web development. The study focuses on issues of jurisdictional dependence, data localization, and potential indirect financing of the aggressor state through digital service payments [1]. Ethical challenges are examined from the perspective of digital sovereignty and responsible design, emphasizing the necessity of transparent and accountable technological ecosystems. The research integrates concepts of normative digital sovereignty (Roberts, 2024) and rights-based digital governance (Fratini, 2024), applying them to the analysis of web infrastructure in Ukraine.

A comparative evaluation of several popular platforms — Webflow, WordPress, Carrd, and HTML/JS development — is conducted according to key ethical and security criteria: jurisdiction, user control, data exportability, transparency, and risk of external interference. The analysis demonstrates that Tilda, despite its technical simplicity, poses critical ethical and information security threats due to its partial connection with Russian jurisdiction and limited user data control. In contrast, open-source or Western-hosted solutions provide higher transparency and resilience against censorship or data leakage.

The findings confirm that adopting ethically neutral and transparent platforms is both a technological and strategic priority for Ukraine. Such a transition not only enhances data protection and independence but also aligns with the broader global movement for ethical digital ecosystems. The article concludes that fostering a culture of ethical web development contributes to national information security, supports innovation, and reinforces Ukraine's position in the international digital space [1]; [3; 6, pp. 10–11].

Keywords*: web platforms, digital ethics, Tilda, Webflow, WordPress, digital sovereignty, information security, ethical design.*

Стаття надійшла до редакції 06.10.2025.
Received 06.10.2025.