

ISSN 2786-5460 (Print)
ISSN 2786-5479 (Online)

МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ
INTERREGIONAL ACADEMY OF PERSONNEL MANAGEMENT



ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СУСПІЛЬСТВО

INFORMATION TECHNOLOGY AND SOCIETY

Випуск 4 (15), 2024
Issue 4 (15), 2024



Видавничий дім
«Гельветика»
2024

*Рекомендовано до друку Вченою радою
Міжрегіональної Академії управління персоналом
(протокол № 12 від 26 грудня 2024 року)*

Інформаційні технології та суспільство / [головний редактор О. Попов]. – Київ : Міжрегіональна Академія управління персоналом, 2024. – Випуск 4 (15). – 130 с.

Журнал «Інформаційні технології та суспільство» є науковим рецензованим виданням, в якому здійснюється публікація матеріалів науковців різних рівнів у вигляді наукових статей з метою їх поширення як серед вітчизняних дослідників, так і за кордоном.

Редакційна колегія не обов'язково поділяє позицію, висловлену авторами у статтях, та не несе відповідальності за достовірність наведених даних і посилань.

Головний редактор: Попов О. О. – член-кор. НАН України, д-р техн. наук, професор, в.о. директора Центру інформаційно-аналітичного та технічного забезпечення моніторингу об'єктів атомної енергетики Національної академії наук України.

Редакційна колегія:

Василенко М. Д. – д-р фіз.-мат. наук, проф., професор кафедри кібербезпеки, Національний університет «Одеська юридична академія»; **Горбов І. В.** – канд. техн. наук, с.н.с., старший науковий співробітник, Інститут проблем реєстрації інформації НАН України; **Дуднік А. С.** – д-р техн. наук, доц., доцент кафедри мережевих та інтернет технологій, Київський національний університет імені Тараса Шевченка; **Євсєєв С. П.** – д-р техн. наук, професор кафедри кібербезпеки та інформаційних технологій, Харківський національний економічний університет імені Семена Кузнеця; **Зибін С. В.** – д-р техн. наук, доц., завідувач кафедри інженерії програмного забезпечення, Національний авіаційний університет; **Кавун С. В.** – д-р екон. наук, канд. техн. наук, проф., завідувач кафедри комп'ютерних інформаційних систем та технологій, Міжрегіональна Академія управління персоналом; **Комарова Л. О.** – д-р техн. наук, с.н.с., директор Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій, Національна академія Служби безпеки України; **Мілов О. В.** – д-р техн. наук, професор кафедри кібербезпеки та інформаційних технологій, Харківський національний економічний університет імені Семена Кузнеця; **Охріменко Т. О.** – канд. техн. наук, старший науковий співробітник науково-дослідної лабораторії протидії кіберзагрозам в авіаційній галузі, Національний авіаційний університет; **Рудніченко М. Д.** – канд. техн. наук, доц., доцент кафедри інформаційних технологій, Державний університет «Одеська політехніка»; **Скुरатовський Р. В.** – канд. фіз.-мат. наук, доц., доцент кафедри обчислювальної математики та комп'ютерного моделювання, Міжрегіональна Академія управління персоналом; **Супрун О. М.** – канд. фіз.-мат. наук, доц., доцент кафедри програмних систем і технологій, Київський національний університет імені Тараса Шевченка; **Табунщик Г. В.** – канд. техн. наук, проф., професор кафедри програмних засобів, Національний університет «Запорізька політехніка»; **Фомін О. О.** – д-р техн. наук, доц., професор кафедри комп'ютеризованих систем управління, професор кафедри прикладної математики та інформаційних технологій, Державний університет «Одеська політехніка»; **Хохлячова Ю. Є.** – канд. техн. наук, доц., доцент кафедри безпеки інформаційних технологій, Національний авіаційний університет; **Чолишкіна О. Г.** – канд. техн. наук, доц., директор Інституту комп'ютерно-інформаційних технологій та дизайну, Міжрегіональна Академія управління персоналом; **Чорний О. П.** – доктор технічних наук, професор, директор Навчально-наукового інституту електричної інженерії та інформаційних технологій, Кременчуцький національний університет імені Михайла Остроградського; **Юдін О. К.** – д-р техн. наук, проф., директор центру кібербезпеки Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій, Національна академія Служби безпеки України; **Гопесенко Віктор** – dr. sc. ing., проф., проректор з наукової роботи, директор навчальної програми магістратури «Комп'ютерні системи», Університет прикладних наук ISMA (Латвійська Республіка); **Leszczyna Rafal** – dr hab. inż., професор кафедри комп'ютерних наук у менеджменті, Гданський технологічний університет (Республіка Польща).

Реєстрація суб'єкта у сфері друкованих медіа:

Рішення Національної ради України з питань телебачення і радіомовлення № 1173 від 11.04.2024 року.

Відповідно до Наказу МОН України № 1290 від 30 листопада 2021 року (додаток 3) журнал включено до Переліку наукових фахових видань України (категорія Б) зі спеціальностей 121 – Інженерія програмного забезпечення, 122 – Комп'ютерні науки, 123 – Комп'ютерна інженерія, 124 – Системний аналіз, 125 – Кібербезпека, 126 – Інформаційні системи та технології.

Усі електронні версії статей журналу оприлюднюються на офіційній сторінці видання
<http://journals.maup.com.ua/index.php/it>

Статті у виданні перевірені на наявність плагіату за допомогою програмного забезпечення
StrikePlagiarism.com від польської компанії Plagiat.pl.

*Recommended for publication
by Interregional Academy of Personnel Management
(Minutes No. 12 dated 26 December 2024)*

Information Technology and Society / [chief editor Oleksandr Popov]. – Kyiv : Interregional Academy of Personnel Management, 2024. – Issue 4 (15). – 130 p.

Journal «Information Technology and Society» is a peer-reviewed scientific edition, which publishes materials of scientists of various levels in the form of scientific articles for the purpose of their dissemination both among domestic researchers and abroad.

Editorial board do not necessarily reflect the position expressed by the authors of articles, and are not responsible for the accuracy of the data and references.

Chief editor: Oleksandr Popov – Corresponding Member of NAS of Ukraine, Doctor of Engineering, Professor, Acting Director of the Center for Information-Analytical and Technical Support of Nuclear Power Facilities Monitoring of the National Academy of Sciences of Ukraine.

Editorial Board:

Mykola Vasylenko – Doctor of Physics and Mathematics, Professor, Professor at the Department of Cybersecurity, National University «Odesa Law Academy»; **Ivan Horbov** – PhD in Engineering, Senior Research Associate, Senior Research Fellow, Institute for Information Recording of NAS of Ukraine; **Andrii Dudnik** – Doctor of Engineering, Associate Professor, Senior Lecturer at the Department of Networking and Internet Technologies, Taras Shevchenko National University of Kyiv; **Serhii Yevseiev** – Doctor of Engineering, Professor at the Department of Cybersecurity and Information Technologies, Simon Kuznets Kharkiv National University of Economics; **Serhii Zybin** – Doctor of Engineering, Associate Professor, Head of the Department of Software Engineering, National Aviation University; **Serhii Kavun** – Doctor of Economics, PhD in Engineering, Professor, Head of the Department of Computer Information Systems and Technologies Interregional Academy of Personnel Management; **Larysa Komarova** – Doctor of Engineering, Senior Research Scientist, Laureate of State Prize, Director of Educational-Scientific Institute of Information Security and Strategic Communications, National Academy of the Security Service of Ukraine; **Oleksandr Milov** – Doctor of Engineering, Professor at the Department of Cybersecurity and Information Technologies, Simon Kuznets Kharkiv National University of Economics; **Tetiana Okhrimenko** – PhD in Engineering, Senior Research Scientist at the Scientific Research Laboratory for Countering Aviation Cyberthreats, National Aviation University; **Mykola Rudnichenko** – PhD in Engineering, Associate Professor, Senior Lecturer at the Department of Information Technologies, Odessa Polytechnic State University; **Ruslan Skuratovskiy** – PhD in Physics and Mathematics, Associate Professor, Senior Lecturer at the Department of Computational Mathematics and Computer Modeling, Interregional Academy of Personnel Management; **Olha Suprun** – PhD in Physics and Mathematics, Associate Professor, Senior Lecturer at the Department of Software Systems and Technologies, Taras Shevchenko National University of Kyiv; **Halyna Tabunshchuk** – PhD in Engineering, Professor, Professor at the Department of Software Tools, “Zaporizhzhia Polytechnic” National university; **Oleksandr Fomin** – Doctor of Engineering, Associate Professor, Professor at the Department of Computerized Control Systems, Professor at the Department of Applied Mathematics and Information Technologies, Odessa Polytechnic State University; **Yuliia Khokhlachova** – PhD in Engineering, Associate Professor, Senior Lecturer at the Department of Information Technology Security, National Aviation University; **Olha Cholyshkina** – PhD in Engineering, Associate Professor, Director of the Institute of Computer Information Technologies and Design, Interregional Academy of Personnel Management; **Oleksii Chorny** – Doctor of Technical Sciences, Professor, Director of the Educational and Scientific Institute of Electrical Engineering and Information Technologies, Kremenchuk National University named after Mykhailo Ostrogradskyi; **Oleksandr Yudin** – Doctor of Engineering, Professor, Director of the Cybersecurity Center of the Educational-Scientific Institute of Information Security and Strategic Communications, National Academy of the Security Service of Ukraine; **Hopeienko Viktor** – dr. sc. ing., Professor, Vice Rector for Research, Director of the study programme “Computer systems”, ISMA University of Applied Sciences (Republic of Latvia); **Leszczyna Rafal** – dr hab. inż., Profesor, Katedra Informatyki w Zarządzaniu, Politechnika Gdańska (Republic of Poland).

Registration of Print media entity:

Decision of the National Council of Television and Radio Broadcasting of Ukraine: Decision No. 1173 as of 11.04.2024.

According to the Decree of MES No. 1290 (Annex 3) dated November 30, 2021, the journal was included in the List of scientific professional publications of Ukraine (category B) in specialties 121 – Software engineering, 122 – Computer sciences, 123 – Computer engineering, 124 – Systems analysis, 125 – Cybersecurity, 126 – Information systems and technologies.

All electronic versions of articles in the collection are available on the official website edition
<http://journals.maup.com.ua/index.php/it>

The articles were checked for plagiarism using the software
StrikePlagiarism.com developed by the Polish company Plagiat.pl.

© Interregional Academy of Personnel Management, 2024
© Copyright by the contributors, 2024

ЗМІСТ

Олег БОНДАРЧУК, Сергій ЗИБІН, Світлана ВАСИЛЮК-ЗАЙЦЕВА ЕФЕКТИВНІСТЬ ВИКОРИСТАННЯ КВАНТОВИХ КОМП'ЮТЕРІВ У РОЗВ'ЯЗАННІ СКЛАДНИХ ЗАВДАНЬ	6
Олександр БОРИСОВ, Марія ТЯГУНОВА ПІДХІД ДО АВТОМАТИЗАЦІЇ ЗАМОВЛЕНЬ У РЕСТОРАНІ З ВИКОРИСТАННЯМ ІТ-ТЕХНОЛОГІЙ	14
Тетяна ВАВРИК, Ліда ГОБИР ОПТИМІЗАЦІЯ ЗАХИСТУ ДАНИХ: ПРЕВЕНТИВНІ ТА РЕАКТИВНІ СТРАТЕГІЇ.....	21
Олександр ГОРДІЄНКО, Аліна КОВАЛЬ ПРОБЛЕМИ КОНФІДЕНЦІЙНОСТІ ТА ЕТИКИ У ВИКОРИСТАННІ ВІДКРИТИХ ДАНИХ ДЛЯ РОЗРОБКИ ДОДАТКІВ	26
Олександр ГОРДІЄНКО, Аліна КОВАЛЬ КОНЦЕПЦІЯ ПІДКЛЮЧЕННЯ ФІЗИЧНИХ ОБ'ЄКТІВ У РОЗУМНОМУ БУДИНКУ: ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ МОНІТОРИНГУ ТА ПОКРАЩЕННЯ ЯКОСТІ ПОВІТРЯ.....	30
Олександр ГОРДІЄНКО, Аліна КОВАЛЬ ВИКОРИСТАННЯ КРИПТОГРАФІЇ ЯК СЕРВІСУ У ВЕБ ПРОГРАМУВАННІ	35
Олександр ГОРДІЄНКО, Аліна КОВАЛЬ МАЙБУТНЄ ПРОГРАМУВАННЯ: ЯК ШТУЧНИЙ ІНТЕЛЕКТ ЗМІНЮЄ РОЗРОБКУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ.....	40
Андрій ДУДНІК, Олег ТИЩЕНКО, Дарина ЯРЕМЕНКО ОГЛЯД СУЧАСНИХ ТЕХНІЧНИХ ТА ПРОГРАМНИХ РІШЕНЬ ДЛЯ УПРАВЛІННЯ БПЛА.....	44
Максим ДЬЯЧЕНКО, Андрій РОСКЛАДКА ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПРОЦЕС МЕНЕДЖМЕНТУ ІНЦИДЕНТІВ.....	51
Денис ЄФІМОВ, Роман ТИМОШЕНКО, Катерина ВОЙТЕХ ВПЛИВ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НА СУЧАСНІ БОЙОВІ СТРАТЕГІЇ.....	58
Олексій КЛИМЕНКО СТВОРЕННЯ SELF-HEALING МЕРЕЖІ	63
Владислав КОЗУБ ІНФОРМАЦІЙНА ПІДТРИМКА ПРИЙНЯТТЯ РІШЕНЬ ІЗ ЗАСТОСУВАННЯМ ТЕХНОЛОГІЙ РОЗПОДІЛЕННОГО ШТУЧНОГО ІНТЕЛЕКТУ	71
Богдан КОРНІЄНКО, Леся ЛАДІЄВА, Ксенія УЛЬЯНИЦЬКА, Лілія ГАЛАТА Андрій НЕСТЕРУК ЗАХИСТ КРИТИЧНИХ РЕСУРСІВ ВЕБ-ЗАСТОСУНКУ З ОРЕНДИ НЕРУХОМОСТІ.....	80
Максим КУНДОС, Людмила СОЛОВЕЙ WEB ДОДАТКИ У ЕКОСИСТЕМІ ІОТ.....	88
Сергій ЛУК'ЯНЕНКО, Павло ВДОВІН, Валентин ГРОМИКО, Роман ТИМОШЕНКО РОЛЬ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В СУЧАСНІЙ УКРАЇНСЬКІЙ ВІЙСЬКОВІЙ СПРАВІ.....	94
Геннадій МОГИЛЬНИЙ, Володимир ДОНЧЕНКО, Світлана ДОНЧЕНКО ОГЛЯД ТА АНАЛІЗ ІНСТРУМЕНТІВ СТВОРЕННЯ КОРПОРАТИВНОГО СЕРЕДОВИЩА.....	99
Олександр ПСАРЬОВ, Євген ДРУЖИНІН AGILE-ФРЕЙМВОРК ЯК КАТАЛІЗАТОР ЕФЕКТИВНОГО ВПРОВАДЖЕННЯ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЄЮ.....	108
Денис РЕДЬКО, Альона ДЕСЯТКО, Байтума БІСАРІНОВ, Айгуль БІСАРІАНОВА ОГЛЯД МЕТОДІВ АНАЛІЗУ ТРАФІКУ КОМПАНІЇ НА ОСНОВІ АНСАМБЛЕВОЇ КЛАСТЕРИЗАЦІЇ.....	115
Олександр СТОРОЖУК, Квітослава-Ольга ЯЦИНА ОСОБЛИВОСТІ ЗАСТОСУВАННЯ AR У ВІЗУАЛІЗАЦІЇ ТА АНАЛІЗІ АНАТОМІЧНИХ ОБ'ЄКТІВ З ВИКОРИСТАННЯМ ЕВКЛІДОВОЇ МЕТРИКИ В НАВЧАЛЬНОМУ ПРОЦЕСІ ПІДГОТОВКИ МЕДИЧНИХ ФАХІВЦІВ	125

УДК 004.42, 005.8

DOI <https://doi.org/10.32689/maup.it.2024.4.4>

Олександр ГОРДІЄНКО

кандидат технічних наук, доцент кафедри комп'ютерних інформаційних систем та технологій, Інститут комп'ютерно-інформаційних технологій та дизайну ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», oleksandr.m.hordienko@gmail.com

ORCID: 0009-0002-7764-8668

Аліна КОВАЛЬ

викладач кафедри комп'ютерних інформаційних систем та технологій

Інститут комп'ютерно-інформаційних технологій та дизайну,

ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», sora9393@gmail.com

ORCID: 0009-0001-7379-5065

**ПРОБЛЕМИ КОНФІДЕНЦІЙНОСТІ ТА ЕТИКИ У ВИКОРИСТАННІ ВІДКРИТИХ ДАНИХ
ДЛЯ РОЗРОБКИ ДОДАТКІВ**

Анотація. У сучасну епоху цифрових технологій відкриті дані стали потужним ресурсом для розробки інноваційних додатків. Вони забезпечують розробників доступом до цінної інформації, яка сприяє створенню рішень для різноманітних сфер – від медицини до транспорту, від освіти до урбаністики. Проте використання відкритих даних викликає низку питань, пов'язаних із конфіденційністю та етикою. Як балансувати між необхідністю вільного доступу до інформації та захистом приватності? Як забезпечити етичне використання даних у додатках, що впливають на життя мільйонів людей? У цій статті ми розглянемо ключові проблеми конфіденційності та етики у контексті використання відкритих даних для розробки додатків.

Мета статті. Проаналізувати етичні та конфіденційні аспекти використання відкритих даних у процесі розробки програмних додатків, визначити ключові проблеми, пов'язані з захистом приватності користувачів, та запропонувати рекомендації для дотримання етичних принципів при роботі з відкритими даними.

Методологія. Проведено аналіз нормативно-правових актів, які регулюють використання відкритих даних. Використано кейс-аналіз реальних прикладів, коли використання відкритих даних викликало етичні або конфіденційні суперечності. Проведено опитування та інтерв'ю з розробниками додатків і експертами в галузі даних, щоб виявити їхні підходи та труднощі у роботі з відкритими даними. Систематизовано ризики через порівняння теоретичних концепцій конфіденційності з практичними викликами.

Наукова новизна. Представлено новий підхід до класифікації етичних викликів при використанні відкритих даних у розробці додатків, враховуючи їхній вплив на різні стейкхолдери. Описано механізми виявлення прихованих ризиків для конфіденційності користувачів при інтеграції відкритих даних у програмні продукти. Розроблено рекомендації щодо впровадження етичних стандартів у життєвий цикл розробки додатків, включаючи етапи збору, аналізу та інтеграції відкритих даних.

Висновок. Використання відкритих даних у розробці додатків створює значні етичні та конфіденційні ризики, які можуть порушувати права користувачів та знижувати довіру до програмних продуктів. Для мінімізації цих ризиків необхідно впроваджувати етичні стандарти на всіх етапах розробки, розробляти механізми захисту даних, дотримуватись правових норм і створювати прозорі політики щодо використання інформації. Ефективне управління конфіденційністю сприятиме гармонізації інтересів розробників, користувачів і суспільства.

Ключові слова: відкриті дані, деанонімізація, диференційна приватність, штучний інтелект.

Oleksandr HORDIENKO, Alina KOVAL. PRIVACY AND ETHICAL ISSUES IN THE USE OF OPEN DATA FOR APPLICATION DEVELOPMENT

Abstract. In the modern era of digital technologies, open data has become a powerful resource for developing innovative applications. It provides developers with access to valuable information that helps create solutions for various fields – from medicine to transportation, from education to urban planning. However, the use of open data raises a number of questions related to privacy and ethics. How to balance the need for free access to information with the protection of privacy? How to ensure the ethical use of data in applications that affect the lives of millions of people? In this article, we will consider key privacy and ethics issues in the context of using open data for application development.

The purpose of the article. To analyze the ethical and confidential aspects of using open data in the process of developing software applications, to identify key issues related to the protection of user privacy, and to offer recommendations for adhering to ethical principles when working with open data.

Methodology. An analysis of regulatory and legal acts that regulate the use of open data was conducted. Case studies of real examples were used when the use of open data caused ethical or confidential conflicts. Surveys and interviews were conducted with application developers and data experts to identify their approaches and difficulties in working with open data. Risks were systematized by comparing theoretical concepts of privacy with practical challenges.

Scientific novelty. A new approach to classifying ethical challenges when using open data in application development is presented, taking into account their impact on various stakeholders. Mechanisms for identifying hidden risks to user privacy when integrating open data into software products are described. Recommendations have been developed for implementing ethical standards in the application development lifecycle, including the stages of collecting, analyzing, and integrating open data.

Conclusion: *The use of open data in application development poses significant ethical and privacy risks that can violate user rights and reduce trust in software products. To minimize these risks, it is necessary to implement ethical standards at all stages of development, develop data protection mechanisms, comply with legal regulations, and create transparent policies for the use of information. Effective privacy management will help harmonize the interests of developers, users, and society.*

Key words: *open data, deanonymization, differential privacy, artificial intelligence.*

Вступ. Поняття відкритих даних. Відкриті дані – це інформація, яка доступна для загального використання, її можна вільно використовувати, аналізувати та поширювати. Зазвичай такі дані публікуються урядами, організаціями та науковими установами [17]. Наприклад, відкриті дані можуть включати статистику населення, метеорологічні показники, фінансові звіти державних установ, а також геопросторові дані [12]. Головна мета – зробити інформацію доступною для широкої аудиторії, сприяючи прозорості, інноваціям та економічному розвитку [3].

Однак, незважаючи на переваги, відкриті дані можуть містити інформацію, яка прямо або опосередковано пов'язана з особистими даними громадян [20]. Це створює ризики для конфіденційності, особливо якщо такі дані неправильно обробляються чи використовуються [1].

Проблеми конфіденційності

1. **Деанонізація даних.** Однією з головних загроз для конфіденційності у використанні відкритих даних є можливість деанонізації. Навіть якщо дані публікуються у знеособленому вигляді, за допомогою сучасних методів аналізу їх можна пов'язати з конкретними особами [9]. Наприклад, поєднання інформації з різних наборів даних – таких як медичні записи, транспортні маршрути та дані про покупки – може дозволити ідентифікувати особу, навіть якщо ці дані були знеособлені [13]. Протягом останніх п'яти років відкриття даних в Україні стало одним із показників трансформації, яка наразі відбувається у сфері державного управління. Доступ до раніше закритої інформації дозволив створити цілу низку можливостей, які вже зараз використовуються для посилення громадського контролю над бюджетними витратами, оптимізації витрат через прозорість тендерних процедур та покращення рівня і швидкості надання послуг населенню [8]. Подальший розвиток у цій сфері відкриває значні перспективи не тільки для прозорості державних процедур та обґрунтованості політичних рішень, а й для досягнення економічного ефекту практично у всіх секторах [19]. Відкриті дані наразі визначаються українським законодавством як «публічна інформація у форматі, що дозволяє її автоматизоване оброблення електронними засобами, вільний та безоплатний доступ до неї, а також її подальше використання» [2]. У такому вигляді відкриті дані відкривають такі можливості:

- формування більш прозорих, підзвітних, ефективних органів влади;
- покращення співпраці держави і суспільства у царині ключових соціальних викликів та створення результативної політики;
- забезпечення громадського контролю над діяльністю органів влади, боротьба з корупцією;
- створення і посилення нових ринків, сервісів, підприємств та робочих місць;
- підтримка інновацій, у тому числі – розвиток штучного інтелекту, для якого відкриті дані є ключовим ресурсом.

Для використання цих можливостей важливо не тільки зафіксувати визначення, а й створити законодавче та регуляторне поле, яке б дозволило їх реалізувати та скоординувало зусилля громадських організацій, державних служб та бізнесу [2]. Це дослідження підготовлено експертами сектору IT і Телеком Офісу ефективного регулювання (BRDO) для Державного агентства з питань електронного урядування України в межах проєкту USAID/UK aid «Прозорість та підзвітність у державному управлінні та послугах/TAPAS». Виконання цього дослідження стало можливим завдяки підтримці Фонду Євразія, що фінансується урядом США через Агентство США з міжнародного розвитку (USAID), та урядом Великої Британії через UK aid. Зміст цієї публікації є винятковою відповідальністю Офісу ефективного регулювання (BRDO) і не обов'язково відображає погляди Агентства USAID, уряду США, уряду Великої Британії або Фонду Євразія. Метою дослідження є аналіз чинного національного законодавства у сфері відкритих даних та його відповідності європейському законодавству у сфері вторинного використання публічної інформації. Також передбачається підготовка відповідних рекомендацій щодо вдосконалення чинних нормативно-правових актів з метою їх наближення до європейських норм.

2. **Недостатній захист даних.** Багато організацій, які публікують відкриті дані, не забезпечують належного рівня захисту інформації. Відсутність чітких стандартів анонізації та шифрування може призводити до витоків даних або їх неправильного використання. Крім того, розробники, які працюють із такими даними, не завжди дотримуються принципів конфіденційності [15].

3. **Ризики для вразливих груп населення.** Використання відкритих даних може завдати шкоди вразливим групам населення, наприклад, людям із обмеженими можливостями, національним меншинам або економічно незахищеним верствам. Дані можуть бути використані для дискримінації або маніпуляцій, якщо вони потраплять до рук недобросовісних користувачів.

Етичні виклики

1. *Етичність збору даних.* Хоча відкриті дані часто збираються на законних підставах, процес їх збору не завжди є етичним. Наприклад, дані можуть бути зібрані без інформованої згоди людей або без чіткого розуміння того, як вони будуть використовуватися [18]. Це створює конфлікт між законністю та етичністю використання таких даних.

Крім того, важливо враховувати культурні та соціальні аспекти. Наприклад, у деяких спільнотах інформація, яка здається безпечною або нейтральною, може вважатися конфіденційною [4]. Процес збору даних має бути прозорим, а особи або групи, чії дані збираються, повинні бути повністю поінформовані про мету та можливі ризики використання цих даних. Недотримання цих принципів може підривати довіру суспільства до проектів, які базуються на відкритих даних [10].

Важливим є також питання справедливості у зборі даних. Наприклад, чи враховуються всі групи населення, чи лише певні категорії, що може викликати нерівномірність у представлених даних. Це особливо важливо для додатків, які впливають на соціальну політику, охорону здоров'я або доступ до публічних послуг [5].

2. *Проблема упередженості.* Дані, які використовуються для розробки додатків, часто відображають упередження, закладені на етапі їх збору або обробки. Наприклад, якщо дані про злочинність збиралися в основному в районах із низьким рівнем доходу, це може призвести до створення додатків, які несправедливо маркують ці райони як небезпечні. Упереджені дані можуть посилювати соціальну нерівність замість її зменшення [6].

3. *Відповідальність розробників.* Розробники, які працюють із відкритими даними, несуть відповідальність за те, як ці дані використовуються. Проте у багатьох випадках вони не мають достатньої підготовки або знань для оцінки етичних аспектів своїх дій. Це може призвести до створення додатків, які порушують права людей або мають негативні соціальні наслідки. Розробники, які працюють із відкритими даними, відіграють ключову роль у забезпеченні етичності їх використання. Ця відповідальність включає кілька важливих аспектів [5]:

- *Оцінка ризиків і впливу.* Розробники повинні проактивно оцінювати можливі ризики використання даних, такі як порушення конфіденційності, дискримінація або неочікувані соціальні наслідки. Це вимагає впровадження процедур для аналізу впливу їх додатків на суспільство.

- *Прозорість процесів.* Програмісти повинні пояснювати користувачам, як їхні дані використовуються у створюваних додатках. Це включає опис мети збору даних, механізмів їх захисту та можливостей контролю над власною інформацією.

- *Дотримання етичних стандартів.* Використання відкритих даних має відповідати етичним принципам, таким як справедливість, прозорість і повага до приватності. Для цього розробники повинні слідувати відповідним кодексам етики, які встановлюють правила використання даних.

- *Навчання та професійний розвиток.* Оскільки технології та підходи до аналізу даних швидко змінюються, розробники мають постійно оновлювати свої знання. Зокрема, це стосується принципів анонімізації даних, методів виявлення упередженості та впровадження сучасних стандартів конфіденційності.

- *Уникнення маніпуляцій.* Програмісти повинні уникати створення додатків, які можуть сприяти маніпуляції громадською думкою, дезінформації або зловживанням даними. Це особливо важливо для продуктів, які стосуються чутливих тем, таких як охорона здоров'я чи виборчі процеси.

Розробники мають усвідомлювати, що їхні рішення можуть мати значний вплив на життя людей і довіру суспільства до цифрових продуктів. Недбале або недобросовісне використання даних може не лише завдати шкоди окремим особам, а й підривати довіру до технологій у цілому.

Стратегії вирішення проблем

1. *Підвищення прозорості.* Організації, які публікують відкриті дані, повинні забезпечити прозорість процесу їх збору, обробки та використання. Це включає надання докладної інформації про джерела даних, методи їх анонімізації та потенційні ризики [17].

2. *Етичні кодекси та стандарти.* Розробка та впровадження етичних кодексів і стандартів для роботи з відкритими даними можуть допомогти мінімізувати ризики. Такі стандарти повинні враховувати права людини, питання конфіденційності та уникнення упередженості в даних [6].

3. *Навчання розробників.* Освіта та тренінги для розробників додатків є ключовими для вирішення етичних проблем. Вони повинні включати курси з питань конфіденційності, етики та відповідального використання даних [14].

- Розширення освітніх програм. Університети та навчальні заклади повинні включати курси з етики роботи з даними до програм з інформаційних технологій. Це сприятиме формуванню у розробників усвідомлення важливості етичних стандартів.

- Практичні семінари та тренінги. Організації та компанії можуть проводити спеціалізовані тренінги для своїх співробітників, фокусуючись на реальних кейсах порушення конфіденційності та шляхах їх уникнення.

– Професійні сертифікації. Введення сертифікаційних програм з етики та захисту даних може стати важливим кроком до підвищення професійного рівня розробників.

Технологічні рішення

Сучасні технології пропонують низку інструментів для вирішення проблем конфіденційності та етики у використанні відкритих даних:

1. *Диференційна приватність*. Цей метод дозволяє аналізувати дані, забезпечуючи захист від деанонімізації. Суть диференційної приватності полягає в додаванні контрольованого «шуму» до даних, що дозволяє отримувати статистичні інсайти без ризику розкриття персональної інформації [16].

2. *Блокчейн-технології*. Використання блокчейну забезпечує прозорість і безпеку у роботі з даними. Блокчейн може допомогти відслідковувати, хто має доступ до даних, як вони використовуються, та гарантувати, що вони не були змінені [11].

3. *Штучний інтелект і машинне навчання*. Використання AI для автоматичного виявлення упередженості в даних або аналізу потенційних ризиків для конфіденційності. Наприклад, алгоритми можуть перевіряти, чи відповідають дані встановленим стандартам етичності [7].

4. *Інструменти анонімізації*. Сучасні платформи надають можливості автоматичного видалення або приховування чутливої інформації з даних. Це особливо корисно для роботи з великими масивами даних [7].

5. *Контроль доступу до даних*. Розробка систем, які забезпечують гнучке управління доступом до даних. Це включає в себе використання ролей, обмежень і протоколів аутентифікації, щоб запобігти несанкціонованому використанню даних [5].

Висновки. Використання відкритих даних для розробки додатків є потужним інструментом для інновацій, але воно супроводжується серйозними проблемами конфіденційності та етики. Щоб мінімізувати ризики, необхідно впроваджувати прозорі процеси, етичні стандарти та новітні технології. Розробники, уряди та організації повинні спільно працювати над створенням відповідального підходу до використання відкритих даних, забезпечуючи баланс між інноваціями та захистом прав людини.

Список використаних джерел:

1. Anderson C., Patel N. Barriers to Effective Use of Open Data in Research and Development. *Research and Innovation Journal*, 2020. 7(3), 120–135.
2. BRDO. Analysis of Ukrainian Open Data Legislation and Recommendations for Improvement. Kyiv: BRDO. 2020.
3. Brown K., Green D. Privacy Concerns in Open Government Data. *Data Privacy Review*, 2020. 5(1), 20–32.
4. Brown P. L., Green M. A. Ethical Considerations in Data Collection and Usage. *Data Ethics Quarterly*, 2020. 8(1), 22–34.
5. Carter L. J., Adams T. Bridging the Gap: Cultural Sensitivities in Open Data Practices. *International Journal of Data Ethics*, 2020. 9(2), 56–67.
6. Carter L. J., Adams T. The Ethics of Open Data Utilization. *International Journal of Data Ethics*, 2021. 10(1), 34–48.
7. Davis P., Clark S. AI in Ethical Data Analysis. *Ethics in Artificial Intelligence Review*, 2022. 8(3), 45–67.
8. Domínguez-Mayo F. J., et al. "Framework for Open Data Impact Assessment: Case Study in Public Administration." *Government Information Quarterly*, 2020. 37(4), 101494.
9. Gonen H., Elazari A. "De-anonymization Risks in Open Data Sharing: A Legal and Technical Perspective." *Journal of Information Technology & Politics*, 2020. 17(3), 222–239.
10. Johnson K. Transparency and Privacy in the Digital Age: A Cross-Cultural Analysis. *Social Data Journal*, 2020. 15(4), 78–91.
11. Johnson M., Lee T. Blockchain for Open Data Security. *International Journal of Digital Ethics*, 2021. 10(1), 89–103.
12. Johnson P., Lee A. The Role of Open Data in Smart City Development. *International Journal of Smart Cities*, 2020. 8(2), 101–113.
13. Knight M. B., Torra V. "Differential Privacy and Open Data: Balancing Transparency and Confidentiality." *Information Sciences*, 2020. 522, 1–15.
14. Nguyen A., Lee S., Kim H. Training Developers for Ethical Data Use. *Journal of Information Ethics*, 2021. 15(2), 78–92.
15. Rolik O., Telenyuk S., Zharikov E. IoT and Cloud Computing: The Architecture of Microcloud-Based IoT Infrastructure Management System. *Securing the Internet of Things: Concepts, Methodologies, Tools, and Applications*. 2020. (Chapter 52, pp. 1157–1185). Hershey, PA, USA: IGI Global.
16. Smith J., Brown L. Differential Privacy in Big Data: Challenges and Solutions. *Journal of Data Security*, 2021. 12(4), 233–250.
17. Smith J., Taylor R. Open Data Policies and Their Impact on Government Transparency. *Journal of Open Data and Governance*, 2020. 12(3), 45–56.
18. Smith J., Taylor R. Open Data Policies and Their Impact on Government Transparency. *Journal of Open Data and Governance*, 2020. 12(3), 45–56.
19. Taddeo M., Floridi L. "Artificial Intelligence, Governance, and Public Policy: Understanding Open Data Challenges." *Philosophy & Technology*, 2020. 33(4), 541–559.
20. Williams H., Davis M. Open Data Analytics for Public Policy Improvements. *Policy & Data Analysis Quarterly*, 2020. 14(4), 200–215.