6. Gee J. P. What video games have to teach us about learning and literacy. *Computers in entertainment (CIE*). 2003. 1(1). Pp. 20-20.

7. González-Gonzále C., & Blanco-Izquierdo F. Designing social videogames for educational uses. *Computers & Education*. 2012. 58(1). Pp. 250-262. [in English]

8. Griffiths M. D. The educational benefits of videogames. *Education and health.* 2002. 20(3). Pp. 47-51.

9. Koutsogiannis D., & Adampa V. Videogames and (language) education: Towards a critical post-videogaming perspective. L1-Educational Studies in Language and Literature. 2022. Pp. 1-28.

10. Magana, A. J., Hwang, J., Feng, S., Rebello, S., Zu, T., & Kao, D. Emotional and cognitive effects of learning with computer simulations and computer videogames. *Journal of Computer Assisted Learning*. 2022. 38(3). Pp. 875-891.

11. Molins-Ruano P., Sevilla C., Santini S., Haya P. A., Rodríguez P. & Sacha G. M. Designing videogames to improve students' motivation. *Computers in Human Behavior*. 2014. 31. Pp. 571-579.

12. Núñez-Barriopedro E., Sanz-Gómez Y., & Ravina-Ripoll R. Videogames in education: Benefitsandharms. *Revista Electrónica Educare*. 2020. 24(2). Pp. 240-257.

13. Schutte N. S., Malouff J. M., Post-Gorden J. C., & Rodasta A. L. Effects of playing videogames on children's aggressive and other behaviors. *Journal of Applied Social Psychology.* 1988. 18(5). Pp. 454-460.

REFERENCES

1. Bacalja, A., Nichols, T. P., Robinson, B., Bhatt, I., Kucharczyk, S., Zomer, C., ... & Schnaider, K. (2024). Postdigital videogames literacies: thinking with, through, and beyond James Gee's learning principles. Postdigital Science and Education. 6(4). Pp. 1103-1142. [in English]

2. Bazile, J. A. (2022). An "alternative to the pen"? Perspectives for the design of historiographical videogames. Games and Culture. 17(6). Pp. 855-870. [in English]

3. Brown, H. J. (2014). Videogames and education. Routledge. [in English]

4. Burn, A. (2021). Literature, videogames and learning. Routledge. [in English]

5. Fabricatore, C. (2000). Learning and videogames: An unexploited synergy. [in English]

6. Gee, J. P. (2003). What video games have to teach us about learning and literacy. Computers in entertainment (CIE). 1(1). Pp. 20-20. [in English]

7. González-González, C., & Blanco-Izquierdo, F. (2012). Designing social videogames for educational uses. Computers & Education. 58(1). Pp. 250-262. [in English]

8. Griffiths, M. D. (2002). The educational benefits of videogames. Education and health. 20(3). Pp. 47-51. [in English]

9. Koutsogiannis, D., & Adampa, V. (2022). Videogames and (language) education: Towards a critical post-videogaming perspective. L1-Educational Studies in Language and Literature. Pp. 1-28. [in English]

10. Magana, A. J., Hwang, J., Feng, S., Rebello, S., Zu, T., & Kao, D. (2022). Emotional and cognitive effects of learning with computer simulations and computer videogames. Journal of Computer Assisted Learning. 38(3). Pp. 875-891. [in English]

11. Molins-Ruano, P., Sevilla, C., Santini, S., Haya, P. A., Rodríguez, P., & Sacha, G. M. (2014). Designing videogames to improve students' motivation. Computers in Human Behavior. 31. Pp. 571-579. [in English]

12. Núñez-Barriopedro, E., Sanz-Gómez, Y., & Ravina-Ripoll, R. (2020). Videogames in education: Benefitsandharms. Revista Electrónica Educare. 24(2). Pp. 240-257. [in English]

13. Schutte, N. S., Malouff, J. M., Post-Gorden, J. C., & Rodasta, A. L. (1988). Effects of playing videogames on children's aggressive and other behaviors 1. Journal of Applied Social Psychology. 18(5). Pp. 454-460. [in English]

ВІДОМОСТІ ПРО АВТОРА

ГУДИМА Віталій – аспірант Українського державного університету імені Михайла Драгоманова.

Наукові інтереси: використання відеоігор у професійній підготовці майбутніх учителів суспільствознавчих предметів: міжнародний досвід.

INFORMATION ABOUT THE AUTHOR

HUDYMA Vitalii – PHD student at the Ukrainian state university named after Mykhailo Drahomanov.

Scientific interests: the use of video games in the professional training of future social studies teachers: international experience.

Стаття надійшла до редакції 22.08.2025 р.
Стаття прийнята до друку 30.08.2025 р.

УДК 316.77:004
DOI: 10.36550/2415-7988-2025-1-220-525-530

НАСТРАДІН Володимир –
кандидат технічних наук, професор,
професор кафедри професійної підготовки,
документознавства та публічного управління
Українського державного університету
імені Михайла Драгоманова
ORCID: https://orcid.org/0009-0009-7208-6986
e-mail: nastradin@ukr.net

ІНФОРМАЦІЙНА БЕЗПЕКА У СОЦІАЛЬНИХ МЕРЕЖАХ: АНАЛІЗ ЗАГРОЗ ТА МЕХАНІЗМІВ ЗАХИСТУ

У статті досліджується питання інформаційної безпеки у соціальних мережах, проведено аналіз загроз та механізмів захисту у провідних соціальних мережах. Обґрунтовано необхідність підвищення рівня медіаосвіти та кібергігієни користувачів соціальних мереж цифрового простору.

Аналіз наукових праць показує, що в соціальних мереж все більше збільшується роль деструктивного впливу, підвищуються ризики поширення дезінформації, інформаційно-психологічних операцій, кібершахрайства тощо. Незважаючи на чітке визнання людського фактору як джерела загроз і вразливостей, національне законодавство та існуючі дефініції не містять системного

механізму для формування індивідуальної стійкості громадян до цих загроз, що потребує введення та детального дослідження концепції кібергігієни, спроможної забезпечити індивідуальний захист користувачів в інформаційному просторі.

У статті проведено класифікацію інформаційних загроз, проведено аналіз правових засад захисту даних, зокрема європейського та чинного українського законодавства у цій сфері. Запропоновано розширити концепцію інформаційної безпеки за рахунок кібергігієни, як ключового елементу, що формує свідомі та дисципліновані поведінкові навички кінцевих користувачів.

Проведено порівняльний аналіз безпеки та конфіденційності у соціальних мережах Facebook (Meta), Telegram, TikTok. Визначено, що Facebook демонструє найвищий рівень відповідності міжнародним стандартам захисту приватності, найбільш широкий набір засобів кібербезпеки та найбільш розгалужену інфраструктуру для боротьби з маніпуляціями та дезінформацією. Проведено експериментальне дослідження оцінки рівня кібергігієни користувачів соціальних мереж, яке підтвердилщ, що людський фактор є основною вразливістю, оскільки технічні та поведінкові практики захисту ігноруються переважною більшістю респондентів.

Зроблено висновок про те, що потребує подальшого дослідження і постійного моніторингу рівень кібергігієни користувачів, організація дієвої системи медіаосвіти та розробка заходів протидії соціальній інженерії та інформаційно-психологічним операціям у соцмережах.

Ключові слова: *інформаційна безпека, кібербезпека, інтернет-комунікації, соціальні мережі, кібергігієна, медіаосвіта.*

NASTRADIN Volodymyr –
Candidate of Technical Sciences, Professor,
Professor of the Department of Professional Training, Document Studies and Public Administration of the Mykhailo Dragomanov Ukrainian State University
ORCID: https://orcid.org/0009-0009-7208-6986
e-mail: nastradin@ukr.net

INFORMATION SECURITY IN SOCIAL NETWORKS: ANALYSIS OF THREATS AND PROTECTION MECHANISMS

The article examines the issue of information security in social networks, analyzes threats and protection mechanisms in leading social networks. The need to increase the level of media education and cyber hygiene of users of social networks in the digital space is substantiated.

Analysis of scientific works shows that the role of destructive influence is increasingly increasing in social networks, the risks of spreading disinformation, information and psychological operations, cyber fraud, etc. are increasing. Despite the clear recognition of the human factor as a source of threats and vulnerabilities, national legislation and existing definitions do not contain a systematic mechanism for building individual resilience of citizens to these threats. This requires the introduction and detailed study of the concept of cyber hygiene, capable of ensuring individual protection of users in the information space.

The article provides a classification of information threats and an analysis of the legal principles of data protection, in particular, European and current Ukrainian legislation in this area. It is proposed to expand the concept of information security through cyber hygiene as a key element that forms conscious and disciplined behavioral skills of end users.

A comparative analysis of security and privacy on social networks Facebook (Meta), Telegram, TikTok was conducted. It was determined that Facebook demonstrates the highest level of compliance with international privacy protection standards, the widest set of cybersecurity tools, and the most extensive infrastructure to combat manipulation and disinformation. An experimental study was conducted to assess the level of cyber hygiene of social media users, which confirmed that the human factor is the main vulnerability, as technical and behavioral protection practices are ignored by the vast majority of respondents.

It was concluded that the level of cyber hygiene of users, the organization of an effective system of media education, and the development of measures to counter social engineering and information and psychological operations in social networks require further research and constant monitoring.

Keywords: *information security, cybersecurity, internet communications, social networks, cyber hygiene, media education.*

Постановка та обґрунтування актуальності проблеми. У сучасному інформаційному суспільстві ключовими цифровими комунікаціями стали соціальні мережі, серед яких найбільш поширені такі як Facebook, TikTok, Telegram та ін. Насьогодні вони стали важливим інструментом не тільки комунікації, а й формування суспільної думки, цифрової ідентичності, професійного розвитку та маркетингу. В той же час, активне використання соціальних мереж зумовлює нові виклики у сфері інформаційної безпеки та захисту персональних даних. За даними звіту дослідницької компанії DataReportal за 2025 рік, понад 5,2 млрд осіб мають облікові записи принаймні в одній соціальній мережі, а обсяг даних, які щоденно генеруються користувачами, вимірюється петабайтами [1].

Наряду з конструктивним характером впливу соціальних мереж все більше збільшується роль і деструктивного впливу. Створюються умови, при яких значно підвищуються ризики поширення дезінформації, інформаційно-психологічних операцій, кібершахрайства тощо. Окрім того, викликом залишається низький рівень медіаосвіти та кібергігієни користувачів, що робить людський фактор одним із ключових ризиків. Саме тому важливу актуальну роль у сучасному суспільстві відіграє медіаосвіта, значно підвищується її роль в забезпеченні інформаційної безпеки людини, держави, суспільства.

Аналіз останніх досліджень і публікацій. Незважаючи на актуальність теми, в українському законодавстві та науковому колі немає однозначної позиції щодо поняття «інформаційна безпека» через його багатовимірний та міждисциплінарний характер. Законодавці та науковці розглядають інформаційну безпеку у дещо схожих, але різних площинах. **В правовому полі** фокус уваги зосереджений на захисті життєво важливих інтересів людини, суспільства держави від небезпек, що виникають у інформаційному просторі (змістовний вплив інформації). **В технологічній площині** увага фокусується на захисті самої інформації та інфраструктури, що її обробляє. Тут

інформаційна безпека розглядається через призму забезпечення трьох ключових принципів (тріада CIA): конфіденційності (Confidentsality), цілісності (Integrity) та доступності (Availability) інформації незалежно від її форми (цифрової, паперової, усної).

Різниця у фокусах цих площин зумовлює відсутність чіткого розмежування між термінами «інформаційна безпека» та «кібербезпека». Хоча наукова спільнота схиляється до того, що кібербезпека є лише підсистемою (або підмножиною) інформаційної безпеки, сфера дії якої обмежується захистом виключно цифрових систем і мереж від кіберзагроз, ця багатомірність залишає невизначеність, яка потребує подальшого аналізу [2].

В статті 1 Закону України «Про основні засади забезпечення кібербезпеки України» кібербезпека визначається як «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі». Стратегія інформаційної безпеки України, затверджена Указом Президента України від 28 грудня 2021 року № 685/2021, визначає інформаційну безпеку як стан захищеності національних інтересів, конституційних прав і свобод громадян в інформаційній сфері.

Українські науковці приділяють значну увагу дослідженню сутності та різних аспектів понять «інформаційна безпека» та «кібербезпека» (В. Ліпкан, В. Цимбалюк, О. Горбенко, С. Морозов, І. Ткаченко, М. Присяжнюк та ін.). На їх думку інформаційна безпека виступає ширшим поняттям, що охоплює всі аспекти захисту інформації незалежно від її форми – електронної, друкованої чи усної. Її ключовими принципами є конфіденційність, цілісність та доступність. Кібербезпека, в свою чергу, є складовою інформаційної безпеки, орієнтованою виключно на цифрові аспекти. Вони включають в себе: захист комп'ютерних систем, мереж і програмного забезпечення від кібератак, шкідливого програмного забезпечення та інших цифрових загроз.

Незважаючи на чітке визнання людського фактора як джерела загроз і вразливостей [3, 4], національне законодавство та існуючі дефініції не містять системного механізму для формування індивідуальної стійкості громадян до цих загроз. Ці аспекти, в свою чергу, створюють ключову прогалину між масштабною державною стратегією інформаційної безпеки та дійсним технічним захистом на рівні кінцевого користувача. Усунення цієї прогалини потребує введення та детального дослідження концепції кібергігієни, представленої сукупністю поведінкових, когнітивних та комунікаційних навичок та спроможної забезпечити індивідуальний захист користувачів в інформаційному просторі.

Мета статті - провести аналіз загроз та механізмів захисту у провідних соціальних мережах для вдосконалення механізмів забезпечення їх інформаційної безпеки.

Виклад основного матеріалу дослідження. Системний аналіз інформаційної безпеки неможливий без чіткої класифікації загроз. Зважаючи на багатовимірний характер інформаційної безпеки, загрози їй прийнято класифікувати за різноманітними критеріями. Перш за все за все звернемо увагу на класифікацію загроз за видом властивості інформації, що порушується. Це так звана модель, визначена вище, як «тріада CIA». Згідно її *загроза конфіденційності* полягає в доступі неавторизованих сторін до конфіденційної приватної інформації. У будь-якій добре організованій системі кібербезпеки конфіденційність досягається шляхом визначення та забезпечення окремих рівнів доступу до інформації. Це часто означає організацію інформації за різними категоріями залежно від того, кому потрібен доступ до певних даних і наскільки ці дані конфіденційні. Іншими словами, інформація розділяється залежно від того, яка шкода ймовірно буде завдана у разі порушення конфіденційності. *Загроза цілісності* стосується загрози узгодженості, точності та достовірності даних у будь-який час. Це означає порушення захисту даних від зміни або видалення неавторизованими сторонами. І нарешті *загроза доступності* полягає в перешкоджанні легкого та постійного доступу до інформації для уповноважених сторін. Це вимагає ретельного обслуговування апаратного забезпечення, технічної інфраструктури, а також систем, що використовуються для зберігання та відображення даних.

Модель CIA фокусується на об'єкті захисту. Для розробки превентивних заходів, критично ***важливим є аналіз критерію джерела походження загрози.*** Відповідно до цього критерію, загрози поділяються на природні (стихійні лиха, кліматичні зміни), техногенні (збої та аварії апаратури) та штучні (антропогенні) [6].

Антропогенні загрози становлять основну частку всіх загроз інформаційній безпеці в світі. До антропогенних загроз належать: фішинг, злам акаунтів, зараження шкідливим програмним забезпеченням, навмисні чи ненавмисні людські помилки при роботі з інформаційними системами. За характером впливу антропогенні загрози поділяються на ненавмисні (помилки користувачів) і навмисні. Останні створюються людиною абсолютно свідомо і мають на меті несанкціонований доступ, змінення або знищення інформації та дестабілізацію інформаційного середовища. Зважаючи на військову інтервенцію росії в Україну, особливої актуальності набуває такий вид навмисних штучних загроз, як інформаційно-психологічні операції (ІПСО).

Узагальнюючи наведені класифікаційні підходи, можна зробити висновок, що загрози інформаційній безпеці є багатовимірним явищем, яке має технічні, організаційні, соціальні та психологічні аспекти. Їхня природа постійно змінюється під впливом розвитку інформаційних технологій, цифровізації суспільства та зростання обсягів оброблюваних даних.

Аналізуючи кіберзагрози, слід зазначити, що вони набули комплексного характеру. Соціальна інженерія та ІПСО активно експлуатують прогалини у кібергігієні користувачів. Ефективний захист цифрового середовища залежить не тільки від індивідуальної дисципліни, але й від політик безпеки, встановлених самими соціальними платформами. Політики безпеки по суті є механізмами захисту від можливих загроз.

Нами проведено порівняльний аналіз підходів до безпеки та конфіденційності, які застосовуються ключовими соціальними мережами, популярними в Україні: Facebook (Meta), Telegram, TikTok. Аналіз охоплював такі ключові аспекти:

регулювання обробки персональних даних (відповідність GDPR, місце зберігання даних, прозорість збору даних);

технічні інструменти та механізми безпеки (двофакторна автентифікація, шифрування, інструменти виявлення підозрілих входів, визначення ботів та фейкових акаунтів);

модераційні політики та інструменти протидії дезінформації (фактчекінг, алгоритми виявлення ІПСО, прозорість блокувань, можливість масових кампаній впливу, ризики пропаганди).

Порівняльний аналіз свідчить, що Facebook демонструє найвищий рівень відповідності міжнародним стандартам захисту приватності. Платформа офіційно дотримується вимог GDPR, регулярно публікує звіти прозорості, а обробка персональних даних здійснюється в дата-центрах ЄС та США із дотриманням сертифікованих протоколів безпеки.

Telegram декларує мінімальний обсяг збирання даних, однак не розкриває точних місць їхнього зберігання та не забезпечує повної прозорості щодо обробки, що унеможливлює однозначну оцінку рівня відповідності GDPR.

TikTok формально заявляє про відповідність GDPR, проте його діяльність тривалий час перебуває під посиленим наглядом регуляторів через підозри у надмірному зборі даних та можливому доступі до них третіх сторін

У сфері технічного захисту Facebook забезпечує найбільш широкий набір засобів кібербезпеки. Користувачам доступні двофакторна автентифікація, апаратні ключі, контроль активних сесій, а також автоматичні системи виявлення аномальної активності та підозрілих входів. Елементи машинного навчання використовуються для попередження фішингових атак, визначення бот-мереж та нейтралізації шкідливого контенту. Telegram пропонує високий рівень захисту лише у межах секретних чатів, де застосовується наскрізне шифрування. TikTok надає базові інструменти захисту – двофакторну автентифікацію, попередження про підозрілі входи та можливість керування пристроями. Проте платформа не застосовує наскрізне шифрування приватних повідомлень, а її алгоритмічна система рекомендацій залишається непрозорою, що збільшує ризики маніпулятивного впливу.

Порівняльний аналіз модераційних механізмів виявляє, що Facebook має найбільш розгалужену інфраструктуру для боротьби з маніпуляціями, дезінформацією та політичними ІПСО. TikTok активно розвиває власні інструменти модерації, однак їхня ефективність залишається предметом критики, особливо у сфері політично чутливого контенту. Платформа використовує автоматизовані фільтри, але їхня точність недостатня, а затримки у видаленні шкідливої інформації створюють додаткові ризики. Telegram характеризується мінімальною модерацією, оскільки фокусується на свободі комунікації. Закриті групи та канали майже не контролюються центрально, що створює сприятливі умови для поширення дезінформації, пропаганди та координованих операцій впливу.

В сучасних умовах ефективна протидія загрозам неможлива без належного нормативно-правового регулювання, яке визначає правила збору, зберігання, обробки й захисту інформації, а також відповідальність за порушення цих норм. Тому наступним кроком до розуміння механізмів забезпечення інформаційної безпеки є аналіз правових засад захисту даних, зокрема європейського та чинного українського законодавства у цій сфері.

На відміну від технічних засобів, що покликані мінімізувати ризики загрози, правові норми забезпечують баланс між потребою суспільства в доступі до інформації та потребою особистості в збереженні права на приватність. Значне зростання обсягу персональних даних в мережі Інтернет зумовило потребу у формуванні чітких міжнародних і національних стандартів захисту інформації. На даний момент, ключовими документами у цій сфері є Загальний регламент Європейського Союзу про захист даних (General Data Protection Regulation – GDPR), ухвалений Європейським Парламентом і Радою ЄС №2016/679 від 27.04 2016 р. та законодавство України, яке покроково гармонізується з європейським законодавством в контексті Євроінтеграції.

В Україні правові засади захисту персональних даних визначені насамперед Законом України «Про захист персональних даних» № 2297-VI від 01.06.2010 р. (зі змінами). Крім базового закону, питання інформаційної безпеки та захисту приватності регулюються також законами України «Про інформацію», «Про електронні комунікації», «Про основні засади забезпечення кібербезпеки України» а також Стратегією інформаційної безпеки України» від 28.12.2021 р. У цих нормативно-правових актах визначено принципи безпечного функціонування цифрового простору, забезпечення конфіденційності комунікацій та реагування на кіберінциденти. З метою гармонізації українського законодавства з європейським, у 2023 році було схвалено нову редакцію законопроєкту «Про захист персональних даних», розроблену на основі вимог GDPR.

Очевидно, що правове регулювання виконує критичну функцію у системі інформаційної та кібербезпеки. Однак, жодна правова норма, навіть найбільш сувора, не може бути достатньо ефективною у боротьбі з найкритичнішою вразливістю – індивідуальним людським фактором. Жоден закон не може контролювати особисту поведінку

користувача, яка призводить до ненавмисних помилок таких як використання слабких паролів чи відкриття підозрілих вкладень а також до успішної реалізації ІПСО, де цільовий вплив спрямований не на технічну систему, а на когнітивний та психологічний стан користувача.

Право, технології та організації забезпечують зовнішній периметр захисту, проте вони не можуть гарантувати внутрішньої стійкості окремої особи. Саме тому, для досягнення цілісного захисту в умовах гібридної війни, коли домінує маніпуляція, абсолютно необхідно розширити концепцію інформаційної безпеки за рахунок кібергігієни. Відповідно до Національної концепції кібербезпеки України, кібергігієна розглядається як «сукупність дій і навичок, спрямованих на зниження ризиків у кіберпросторі та підтримання належного рівня безпеки інформаційних систем і персональних даних користувачів» [5, 6]. Саме кібергігієна є ключовим елементом, що формує свідомі та дисципліновані поведінкові навички кінцевих користувачів.

Рівень кібергігієни користувачів визначає їх ступінь вразливості до кіберзагроз та психологічних маніпуляцій, зокрема соціальної інженерії, фішингу та інформаційно-психологічних операцій. На практиці все це означає не тільки технічну грамотність, а й свідоме ставлення до власних дій в мережі. Це стосується обміну інформацією в соціальних мережах, дотримання правил конфіденційності, використання двофакторної автентифікації, своєчасного оновлення програмного забезпечення тощо.

Для оцінка рівня кібергігієни користувачів соціальних мереж та виявлення основних ризиків, пов'язаних із недотриманням правил безпечної поведінки в цифровому середовищі нами проведено анонімне опитування серед найбільш активних користувачів соціальних мереж (55 респондентів). Завдання опитування полягали у визначенні: рівня обізнаності користувачів щодо базових принципів кібербезпеки; поширених помилках при роботі з персональними даними; ставлення до політик конфіденційності соціальних мереж; частоти використання захисних механізмів (складні паролі, двофакторна автентифікація, налаштування приватності тощо). Вибіркова сукупність включала користувачів різного віку починаючи з 18 років, які є користувачами соціальних мереж Facebook, Instagram, Telegram, TikTok та інших. У опитуванні взяло участь 67,3% жінок та 32,7% чоловіків. Опитування проводилося в онлайн-форматі за допомогою Google Forms в період з жовтня по листопад 2025 року. Отримані дані підтвердили, що людський фактор є основною вразливістю, оскільки технічні та поведінкові практики захисту ігноруються переважною більшістю респондентів.

Висновки та перспективи подальших розвідок напряму. Інформаційна та кібербезпека в соціальних мережах є багаторівневим явищем. Вона охоплює технічні, організаційні, поведінкові та правові аспекти. Правове регулювання захисту даних відіграє головну роль у формуванні безпечного інформаційного середовища і потребує подальшого вдосконалення. Глибокий аналіз політик безпеки провідних соціальних платформ – Facebook, Telegram і TikTok вказує, що кожна з них має різні рівні відкритості, алгоритми модерації та технічні інструменти захисту. Потребує подальшого дослідження і постійного моніторингу рівень кібергігієни користувачів.

Дієвим механізмом підвищення кібергігієни користувачів слугують організаційно-технічні заходи, серед яких: регулярне оновлення паролів, багатофакторна автентифікація, використання менеджерів паролів, посилення налаштувань приватності, критична оцінка інформації, перевірка джерел та уникнення підозрілих контактів тощо. Особливої уваги в подальшому потребують наукові доробки щодо протидії соціальній інженерії та інформаційно-психологічним операціям у соцмережах.

СПИСОК ДЖЕРЕЛ

1. Буняк Н. М. Соціальна безпека людини: сутність та шляхи забезпечення. *Економіка і суспільство*. Вип. №37. 2022. С. 27-33.

2. Горбенко О. І. Інформаційна та кібербезпека: концептуальні засади та практичні аспекти. Харків: Фоліо, 2017. 320 с.

3. Довгань О. Д. Правові засади формування і розвитку системи забезпечення інформаційної безпеки України. *Інформаційна безпека людини, суспільства, держави.* 2015. № 3. С. 6-17.

4. Титова Н. М. (та ін.) Інформаційна безпека та кібербезпека держави: навч. посіб. / за заг. ред. М. М. Присяжнюка. Київ : Ліра-К, 2024. 224 с.

5. Розпорядження Кабінету Міністрів України «Про схвалення Концепції розвитку цифрових компетентностей та затвердження плану заходів з її реалізації» від 3 березня 2021 р. № 167-р.

6. Богуш В. М., Богуш В. В., Бровко В. Д., Настрадін В. П. Основи кіберпростору, кібербезпеки та кіберзахисту : навч. посіб. Київ : Видавництво Ліра-К, 2020. 554 с.

REFERENCES

1. Bunjak, N.M. (2022) Social'na bezpeka lyudyny: sutnist' ta shlyakhy zabezpechennya [Human social security: essence and ways of ensuring it]. Ekonomika i suspil'stvo. Vyp. № 37. S. 27-33. [in Ukrainian]

2. Horbenko, O.I. (2017) Informaziyna ta kiberbezpeka: koceptual'ni zasady ta praktychni aspekty. [Information and cybersecurity: conceptual foundations and practical aspects]. Kharkiv. Folio. 320 c. [in Ukrainian]

3. Dovhan' O.D. (2015) Pravovi zasady formuvannya i rozvytku systemy zabezpechennya informatsiinoyi bezpeky Ukrayiny [Legal principles of the formation and development of the information security system of Ukraine]. Informatsiyna bezpeka liudyny, suspil'stva, derzhavy. № 3. S. 6-17. [in Ukrainian]

4. Tytova, N. M. (ta in.) (2024) Informatsiyna bezpeka ta kiberbezpeka derzhavy [Information security and cybersecurity of the state]: navch. posib. / za zah. red. M. M. Prysyazhnyuka. K. Lira-K. 224 s. [in Ukrainian]

5. Rozporyadzhennya Kabinetu Ministriv Ukrayiny (2021) «Pro skhvalennya Kontseptsiyi rozvytku zyfrovykh kompetentnostei ts zatverdzhennya planu zakhodiv z yiyi realizatsiyi» [On the approval of the Concept for the Development of Digital Competencies and the approval of the action plan for its implementation]. Vid 3 bereznya 2021 r. № 167-r. [in Ukrainian]

6. Bohush, V. M., Bohush, V. V., Brovko, V. D., Nastradin, V. P. (2020) Osnovy kiberprostoru, kiberbezpeky

ta kibtrzakhystu [Fundamentals of Cyberspace, Cybersecurity, and Cyberdefense]: navch. posib. Kyyiv : Vydavnytstvo Lira-K. 554 s. [in Ukrainian]

ВІДОМОСТІ ПРО АВТОРА

НАСТРАДІН Володимир – кандидат технічних наук, професор, професор кафедри професійної підготовки, документознавства та публічного управління Українського державного університету імені Михайла Драгоманова.

Наукові інтереси: професійна підготовка фахівців з національної, інформаційної та кібербезпеки, системний аналіз, інформаційно-аналітична та управлінська діяльність.

INFORMATION ABOUT THE AUTHOR

NASTRADIN Volodymyr – Candidate of Technical Sciences, Professor, Professor of the Department of Professional Training, Document Studies and Public Administration of the Mykhailo Dragomanov Ukrainian State University.

Scientific interests: professional training of specialists in national, information and cybersecurity, systems analysis, information and analytical and management activities.

Стаття надійшла до редакції 22.08.2025 р.
Стаття прийнята до друку 30.08.2025 р.