DOI 10.31891/2307-5732-2023-321-3-210-213
УДК 004.773.2

ФЕДУШКО СОЛОМІЯ
Національний університет «Львівська політехніка»
ORCID ID: 0000-0001-7548-5856
e-mail: solomiia.s.fedushko@lpnu.ua

СУЧАСНІ ПІДХОДИ ДО ДОСЛІДЖЕННЯ КІБЕРБЕЗПЕКИ ТА КІБЕРГІГІЄНИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ СУСПІЛЬСТВА

У сучасному цифровому суспільстві кібербезпека та кібергігієна стали вирішальними для захисту людей, організацій та держав від кіберзагроз. У цій статті обговорюється важливість досліджень у галузі кібергігієни та кібербезпеки, які включають розробку нових методів захисту інформаційних технологій та навчання користувачів щодо важливості кібербезпеки. Належні практики кібергігієни, такі як регулярна зміна паролів, використання антивірусного програмного забезпечення та уникнення підозрілих вебсайтів, можуть запобігти несанкціонованому доступу до конфіденційної інформації та зменшити поширення шкідливих програм і вірусів. Представлено всебічний огляд досліджень у галузі кібергігієни та кібербезпеки, які набувають все більшої актуальності в сучасному технологічному світі.

Ключові слова: кібергігієна, кібербезпека, цифрове суспільство, веб-технології, соціальна комунікація.

FEDUSHKO SOLOMIIA
Lviv Polytechnic National University

MODERN APPROACHES TO THE STUDY OF CYBERSECURITY AND CYBER HYGIENE IN THE FRAMEWORK OF DIGITAL TRANSFORMATION OF SOCIETY

In today's digital society, cybersecurity and cyber hygiene have become crucial for safeguarding individuals, organizations, and states from cyber threats. This scientific paper discusses the significance of cyber hygiene and cybersecurity research, which involves developing new methods to protect information technology and educating users on the importance of cybersecurity. The paper highlights the consequences of negative digital technology impacts on human health and the environment and emphasizes the need to develop prevention methods. Good cyber hygiene practices such as changing passwords regularly, using antivirus software, and avoiding suspicious websites can prevent unauthorized access to sensitive information and reduce the spread of malware and viruses. This study stresses the importance of maintaining cyber health for the integrity of computer systems and networks. This paper aims to emphasize the importance of cyber hygiene and cybersecurity in modern society and promote good cyber hygiene practices to protect individuals, organizations, and states from cyber threats. This paper provides a comprehensive overview of cyber hygiene and cybersecurity research, which is increasingly relevant in today's rapidly developing technological world. The paper highlights the consequences of negative digital technology impacts on human health and the environment, emphasizing the need for developing prevention methods. Additionally, the paper emphasizes the importance of cybersecurity at the cultural and educational levels to ensure protection against cyber threats. This paper provides practical recommendations for individuals and organizations to practice good cyber hygiene, including changing passwords regularly, using antivirus software, avoiding suspicious websites, keeping software up to date, and avoiding opening suspicious emails or attachments. Implementing these practices helps protect sensitive information, prevent the spread of malware and viruses, and maintain the overall integrity of computer systems and networks.

Keywords: cyber hygiene, cyber security, digital society, web technology, social communication.

Постановка проблеми

У сучасному світі, що характеризується швидким технологічним розвитком, кібербезпека та кібергігієна стають все більш актуальними питаннями. Це пов'язано зі зростаючою кількістю кібератак, витоків даних, шахрайства в Інтернеті та інших кіберзлочинів, які можуть значно пошкодити як окрему людину, так і велику компанію або державу в цілому. Один з ключових підходів до дослідження кібербезпеки полягає у розробці та впровадженні нових методів захисту інформаційних технологій. Такі методи можуть включати в себе застосування криптографічних технологій, розробку систем ідентифікації та аутентифікації користувачів, а також забезпечення безпеки мережевих протоколів. Інший підхід полягає у забезпеченні кібербезпеки на рівні культури та освіти користувачів інформаційних технологій. Цей підхід передбачає навчання користувачів правилам безпеки в інтернеті, забезпечення їх доступу до інформації про кіберзагрози та методи їх запобігання.

Велика увага приділяється дослідженню кібергігієни [1] – поняттю, яке описує можливі наслідки негативного впливу цифрових технологій на здоров'я людей та навколишнє середовище. Дослідження в цій галузі дозволяють зрозуміти наслідки використання цифрових пристроїв та програм на здоров'я людей та довкілля, а також розробляти методи їх запобігання. Зі зростанням розвитку цифрових технологій кібергігієна [2] та кібербезпека [3] стали важливими аспектами життя сучасного суспільства.

Кібергігієна стосується практик і заходів, яких особи та організації застосовують для підтримки кіберздоров'я [4], тоді як кібербезпека стосується захисту комп'ютерних систем і мереж від несанкціонованого доступу або атак. У цьому дослідження висвітлюється важливість кібергігієни та кібербезпеки в цифровому суспільстві. Кібергігієна важлива з кількох причин. По-перше, вона допомагає окремим особам та організаціям захистити свої конфіденційні дані та інформацію.

У сучасну цифрову епоху інформація – це влада, і кіберзлочинці завжди шукають способи отримати її для своїх зловмисних цілей. Дотримання належної кібергігієни, наприклад, регулярна зміна паролів, використання антивірусного програмного забезпечення та уникнення підозрілих веб-сайтів, може запобігти

несанкціонованому доступу до конфіденційної інформації. По-друге, кібергігієна також може допомогти запобігти поширенню шкідливих програм і вірусів [5]. Шкідливе програмне забезпечення та віруси можуть завдати значної шкоди комп'ютерним системам і мережам, а також легко поширюватися через незахищені системи. Дотримуючись належної кібергігієни, наприклад, оновлюючи програмне забезпечення та уникаючи відкриття підозрілих електронних листів чи вкладень, окремі особи та організації можуть зменшити ризик зараження шкідливим програмним забезпеченням та вірусами.

Кібергігієна важлива для підтримки загальної цілісності комп'ютерних систем і мереж. Неналежні практики кібергігієни можуть послабити безпеку системи, роблячи її вразливою до атак. Впроваджуючи належні практики кібергігієни, окремі особи та організації можуть мінімізувати ризик кібератак і зменшити тяжкість наслідків будь-яких успішних атак, які можуть статися. Кібербезпека також має вагоме значення в цифровому суспільстві. По-перше, кібербезпека допомагає захистити людей та організації від кібератак [6, 7]. Кіберзлочинці постійно розробляють нові способи атак на комп'ютерні системи та мережі, а заходи кібербезпеки, такі як брандмауери, системи виявлення вторгнень та шифрування, можуть допомогти запобігти несанкціонованому доступу або пом'якшити наслідки атаки. По-друге, кібербезпека допомагає підтримувати доступність і функціональність комп'ютерних систем і мереж. Кібератаки можуть спричинити значні перебої в роботі систем і мереж, що призводить до простоїв і зниження продуктивності.

Впроваджуючи ефективні заходи кібербезпеки, організації можуть гарантувати, що їхні системи та мережі залишатимуться працездатними та доступними для користувачів. Кібербезпека важлива для захисту репутації окремих осіб та організацій. Кібератаки можуть завдати шкоди репутації організації, особливо якщо викрадено конфіденційну інформацію або скомпрометовано дані клієнтів. Впроваджуючи ефективні заходи кібербезпеки, організації можуть захистити свою репутацію та зберегти довіру клієнтів.

Метою статті є представлення всебічного огляду досліджень у галузі кібергігієни та кібербезпеки, які набувають все більшої актуальності в сучасному технологічному світі.

Аналіз останніх джерел

Сучасні підходи до дослідження кібербезпеки та кібергігієни є надзвичайно актуальними в умовах швидкого розвитку цифрової трансформації суспільства. У зв'язку з цим, виникає необхідність вивчення та аналізу нових технологій та методів захисту від кіберзагроз. У зв'язку з цим, науковці та фахівці з усього світу працюють над розробкою нових підходів до дослідження кібербезпеки та кібергігієни. Одним з найважливіших напрямків є вивчення цих проблем в умовах цифрової трансформації суспільства, яка відбувається в останні роки. Для знаходження прогалин у дослідженні кібергігієни та кібербезпеки проведено ґрунтовний аналіз наукових публікацій у наукометричній базі Scopus. Результатом аналізу є відбір 93 наукові публікації (рис. 1) за ключовим слово TITLE-ABS-KEY (cyber AND hygiene, AND cyber AND security) [8].

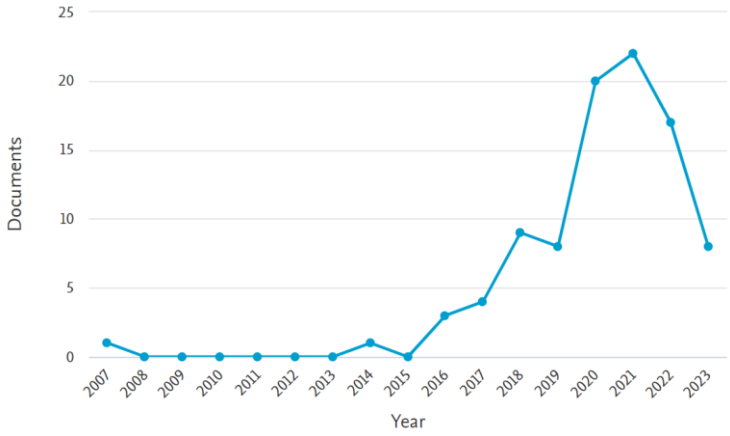

Рис. 1. Статика аналізу досліджень у Scopus за ключовими словами “cyber hygiene”, “cyber security”

На основі аналізу створено візуальну карту цитувань наукових статей [9] у Scopus з тематики кібербезпеки та кібергігієни (рис. 2).

Кібергігієна та кібербезпека є міждисциплінарними галузями, які охоплюють різні дисципліни та напрямки досліджень, включи такі галузі [10]:

- Комп'ютерні науки – вивчення комп'ютерних систем, програмного забезпечення та алгоритмів. Комп'ютерні вчені працюють над розробкою безпечних систем і мереж, а також розробляють нові методи запобігання кібератакам.
- Інформаційні технології – вивчення та використання систем і програмного забезпечення для зберігання, пошуку та передачі інформації. IT-спеціалісти працюють над впровадженням заходів безпеки, управлінням мережами та захистом конфіденційних даних.
- Кібербезпека – захист комп'ютерних систем і мереж від несанкціонованого доступу та кібератак. Фахівці з кібербезпеки працюють над розробкою та впровадженням заходів безпеки, проводять оцінку ризиків та реагують на інциденти, пов'язані з безпекою.
- Криптографія – вивчення кодів і шифрів, що використовуються для забезпечення безпеки комунікації та захисту конфіденційних даних. Криптографи працюють над розробкою нових методів шифрування та аналізують існуючі системи шифрування на наявність вразливостей.
- Управління ризиками – виявлення, оцінку та зменшення ризиків для комп'ютерних систем та мереж. Фахівці з управління ризиками працюють над розробкою політик і процедур для управління та реагування на загрози безпеці.

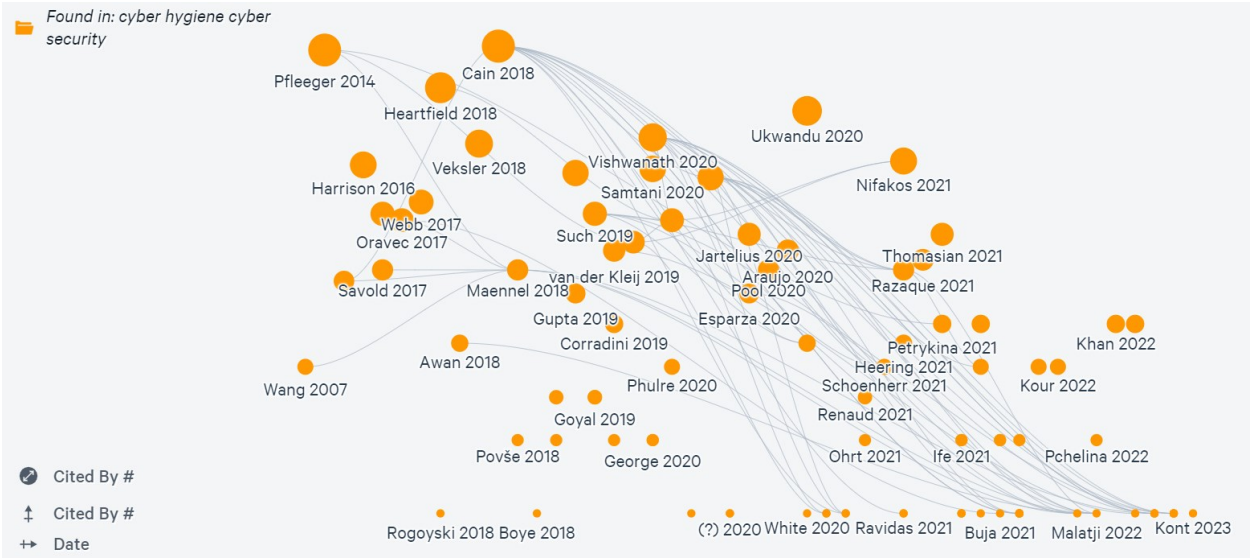

Рис. 2. Візуальна карта цитувань наукових статей у Scopus з тематики кібербезпеки та кібергігієни

- Правоохоронна діяльність – розслідування та переслідування кіберзлочинів. Фахівці правоохоронних органів працюють над розробкою стратегій запобігання кіберзлочинам, а також над виявленням і арештом кіберзлочинців.
- Психологія – вивчення та пізнання людської поведінки. Фахівці з кібербезпеки співпрацюють з психологами, щоб зрозуміти поведінку і мотивацію кіберзлочинців і розробити стратегії запобігання атакам.

Кібергігієна та кібербезпека є міждисциплінарними галузями, які включають різні напрямки досліджень та експертизи. Для ефективного захисту комп'ютерних систем і мереж від кіберзагроз необхідний комплексний підхід.

Виклад основного матеріалу

Кібергігієна та кібербезпека є важливими аспектами сучасного суспільства. Приватні особи та організації повинні впроваджувати належні практики кібергігієни, щоб захистити свою конфіденційну інформацію, запобігти поширенню шкідливих програм і вірусів та підтримувати цілісність своїх комп'ютерних систем і мереж. Вони також повинні впроваджувати ефективні заходи кібербезпеки для запобігання кібератакам, підтримки доступності та функціональності своїх систем і мереж, а також захисту своєї репутації. Оскільки цифрове суспільство продовжує розвиватися, важливість кібергігієни та кібербезпеки буде тільки зростати. Кібергігієна та кібербезпека – це два споріднені поняття у сфері цифрової безпеки, але вони стосуються різних аспектів захисту комп'ютерних систем та мереж від кіберзагроз. Кібергігієна – це сукупність практик і заходів, яких вживають окремі особи та організації для підтримки здоров'я і цілісності своїх цифрових систем і даних. Це включає такі заходи, як оновлення програмного забезпечення та операційних систем, регулярне резервне копіювання важливих даних, використання надійних паролів, уникнення підозрілих електронних листів і веб-сайтів, а також впровадження брандмауерів та інших заходів безпеки. Належна кібергігієна допомагає запобігти кібератакам і мінімізувати шкоду, заподіяну в разі їх здійснення. З іншого боку, кібербезпека стосується ширшої сфери захисту комп'ютерних систем і мереж від зловмисників і кіберзагроз. Сюди входить все – від розробки безпечного програмного та апаратного забезпечення до захисту від спроб хакерських атак, вірусів та інших видів кібератак. Кібербезпека – це безперервний процес, який включає управління ризиками, оцінку вразливостей, планування реагування на інциденти, а також постійний моніторинг і вдосконалення. Таким чином, хоча кібергігієна та кібербезпека (таблиця 1) тісно пов'язані між собою, вони відрізняються за сферою застосування та фокусом. Кібергігієна стосується конкретних практик і заходів для підтримки працездатності цифрових систем, тоді як кібербезпека охоплює ширшу мету захисту комп'ютерних систем і мереж від широкого спектру загроз. Обидва поняття є важливими компонентами комплексного підходу до цифрової безпеки.

Кібергігієна та кібербезпека є критично важливими компонентами забезпечення безпеки в Інтернеті. Кібергігієна зосереджена на індивідуальній поведінці та звичках користувачів, а кібербезпека зосереджена на захисті комп’ютерних систем і мереж від зовнішніх загроз. Обидва важливі для запобігання кібератакам, захисту від витоку даних і крадіжки, а також підтримки загальної безпеки комп’ютерних систем і мереж.

Таблиця 1

Порівняння характеристик кібергігієни та кібербезпеки

Характеристика	Кібергігієна	Кібербезпека
Визначення	Практика підтримки хороших звичок і поведінки для забезпечення безпеки в інтернеті.	Захист комп'ютерних систем, мереж і даних від крадіжки, пошкодження або несанкціонованого доступу.
Область застосування	Зосереджено на індивідуальній поведінці та звичках користувачів.	Зосереджено на захисті комп'ютерних систем і мереж від зовнішніх загроз.
Важливість	Допомагає запобігти кібератакам і поширенню шкідливих програм.	Захищає від витоку даних, крадіжок та інших кіберзлочинів.
Приклади	Оновлюйте програмне забезпечення та антивірусні програми, створюйте надійні паролі та уникайте підозрілих електронних листів або веб-сайтів.	Встановлення систем виявлення вторгнень і програмного забезпечення для шифрування, проведення регулярних перевірок безпеки та впровадження заходів контролю доступу.
Мета	Щоб зменшити ризик кібератак і запобігти поширенню шкідливих програм або вірусів.	Для захисту комп'ютерних систем і даних від несанкціонованого доступу, крадіжки або пошкодження.
Ключові фактори	Регулярні оновлення та технічне обслуговування, освіта та обізнаність, а також відповідальна поведінка у веб.	Оцінка та управління ризиками, планування реагування на інциденти та використання передових заходів безпеки та технологій.

Висновки

Кібергігієна та кібербезпека є критично важливими аспектами цифрового суспільства. Належні практики кібергігієни можуть допомогти окремим особам і організаціям захистити свої конфіденційні дані та запобігти поширенню шкідливих програм і вірусів. Ефективні заходи кібербезпеки можуть запобігти кібератакам, підтримувати доступність і функціональність комп'ютерних систем і мереж, а також захистити репутацію окремих осіб і організацій. Оскільки технології продовжують розвиватися, важливо, щоб окремі особи та організації надавали пріоритет кібергігієні та кібербезпеці, щоб забезпечити цілісність, безпеку та надійність цифрових систем і мереж. Для дослідження кібергігієни та кібербезпеки використовують декілька підходів. Один із підходів полягає в тому, щоб вивчати кібербезпеку та кібергігієну як складові частини більш широкої концепції кібербезпеки та кіберзахисту. Цей підхід дозволяє розглядати ці проблеми з точки зору технологій, процедур та людей, що є складовими частинами кібербезпеки та кібергігієни. Крім того, вивчення цих проблем у контексті більш широкої концепції кібербезпеки дозволяє визначити більш ефективні підходи до їх вирішення. Інший підхід полягає у вивченні кібербезпеки та кібергігієни як соціально-психологічних проблем, та різних аспектів поведінки користувачів в Інтернет.

References

1. Maennel K., Mäses S., Maennel O. Cyber Hygiene: The Big Picture. Lecture Notes in Computer Science. 11252 LNCS. 2018. pp. 291-305. DOI: 10.1007/978-3-030-03638-6_18

2. Ncubukezi T., Mwansa L., Rocaries F. A Review of the Current Cyber Hygiene in Small and Medium-sized Businesses. 2020 15th International Conference for Internet Technology and Secured Transactions. ICITST 2020. DOI: 10.23919/ICITST51030.2020.9351339

3. Meshkat L., Miller R. A Systems Approach for Cybersecurity Risk Assessment. Proceedings - Annual Reliability and Maintainability Symposium. 2022. DOI: 10.1109/RAMS51457.2022.9893966

4. Gupta S., Furnell S. From Cybersecurity Hygiene to Cyber Well-Being. Lecture Notes in Computer Science. 13333. 2022. pp. 124-134. DOI: 10.1007/978-3-031-05563-8_9

5. Vishwanath A., Neo L. Cyber hygiene: The concept, its measure, and its initial tests. Decision Support Systems. 2020. pp. 128. DOI: 10.1016/j.dss.2019.113160

6. Patel S., Doshi N. Internet of Behavior in Cybersecurity: Opportunities and Challenges. Lecture Notes in Electrical Engineering. 936. 2022. pp. 219–227. DOI: 10.1007/978-981-19-5037-7_14

7. Fedushko S., Benova E. Semantic analysis for information and communication threats detection of online service users. Procedia Computer Science. Volume 160. 2019. pp. 254-259. DOI: 10.1016/j.procs.2019.09.465

8. Scopus. URL: https://www.scopus.com.

9. Litmaps. URL: https://app.litmaps.com/map.

10. Cain A., Edwards M., Still J. An exploratory study of cyber hygiene behaviors and knowledge. Journal of Information Security and Applications. 42. 2018. pp. 36–45. DOI: 10.1016/j.jisa.2018.08.002