УДК 004.773.2
DOI https://doi.org/10.51989/NUL.2024.6.8

КІБЕРГІГІЄНА ЯК ЧИННИК ЗАПОБІГАННЯ КІБЕРЗАГРОЗАМ

Красніков Сергій Анатолійович,
orcid.org/0000-0001-6548-5457
провідний науковий співробітник
Українського науково-дослідного інституту спеціальної техніки
та судових експертиз
Служби безпеки України

Стаття присвячена аналізу концепції кібергігієни як ключового елемента запобігання кіберзагрозам. Розглянуто основні принципи кібергігієни, їх вплив на цифрове середовище, а також практичні рекомендації щодо їх впровадження у повсякденну діяльність користувачів. Аналізуються поняття «кібергігієна» та «кібербезпека», досліджується співвідношення цих понять. Обґрунтовується, що кібергігієна становить специфічний набір профілактичних заходів, які кожен користувач має вживати для захисту своїх даних та пристроїв. Обговорюється важливість ключових аспектів кібергігієни, таких як захист особистих даних, протидія фішингу, безпека пристроїв, яка передбачає використання антивірусного програмного забезпечення та оновлення операційної системи. Особливу увагу приділено інформаційним аспектам кібергігієни у контексті критичної інфраструктури та освітніх програм. Зроблено висновок, що розробка внутрішніх політик інформаційної безпеки, проведення регулярних навчань для співробітників і впровадження сучасних технологій кіберзахисту є невід'ємною складовою частиною кібергігієни на рівні організацій. Аналізуються положення чинного законодавства України з питань забезпечення кібербезпеки, зміст якого передбачає підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, засвоєння комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки, підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту. Звертається увага на стратегічні цілі Стратегії кібербезпеки України, які передбачають реформування системи підготовки та підвищення кваліфікації кадрів, а також розробку навчальних програм, курсів, тренінгів з кібернавчання для всіх верств населення. Підкреслюється, що розробка таких освітніх програм сприятиме формуванню у суспільстві звички до безпечної роботи з цифровими технологіями. Зроблено висновок, що інвестиції у навчання та впровадження сучасних технологій дозволять суттєво зменшити ризики кібератак та забезпечити більш безпечне функціонування цифрового середовища.

Ключові слова: *законодавство, кіберзагрози, кібергігієна, кібербезпека, користувачі, критична інфраструктура, цифрова грамотність, освітні програми.*

Krasnikov Serhii. Cyber hygiene as a factor of cyber threats prevention

The article is devoted to the analysis of the concept of cyber hygiene as a key element of preventing cyber threats. The main principles of cyber hygiene, their impact on the digital environment, as well as practical recommendations for their implementation in the daily activities of users are considered.

The concepts of "cyber hygiene" and "cyber security" are analyzed, and the relationship between these concepts is investigated. It is argued that cyber hygiene represents a specific set of preventive measures that each user should follow to protect their data and devices. The importance of key aspects of cyber hygiene is discussed, such as: protection of personal data; anti-phishing; device security, which involves the use of anti-virus software and operating system updates. Particular attention is paid to aspects of cyber hygiene in the context of critical infrastructure and educational programs. It was concluded that the development of internal information security policies, regular training for employees and the introduction of modern protection technologies are an integral part of cyber hygiene at the level of organizations. The provisions of the current legislation on ensuring cyber security are analyzed, the content of which involves increasing the digital literacy of citizens and the culture of safe behavior in cyberspace, assimilation of complex knowledge, skills and abilities necessary to support the goals of cyber security, increasing the level of public awareness of cyber threats and cyber protection.

It was concluded that investments in training, development of policies and implementation of modern technologies will significantly reduce risks and ensure safer functioning of the digital environment.

Key words: *legislation, cyber threats, cyber hygiene, cyber security, digital literacy, educational programs, users, critical infrastructure.*

Постановка проблеми. Нові виклики та загрози, що постали перед Україною у кіберпросторі, зумовлюють зростання ролі кібербезпеки в процесах цифрової трансформації держави. З кожним роком кількість кіберзагроз у світі невпинно зростає. Після повномасштабного вторгнення росії на територію України органи державної влади України стали об'єктами кібератак з боку російських хакерів. Значна частина цих кібератак припадає на об'єкти критичної інформаційної структури, енергетичної сфери та логістики. Водночас кіберпростір України активно використовується ворогом для поширення фейків, дипфейків, підробки сайтів, фішингових атак, заволодіння акаунтами тощо [1, с. 49]. Фахівці з кібербезпеки відзначають: «У все більш оцифрованому світі, де персональні дані є наріжним каменем сучасної економіки, перетин захисту споживачів і кібербезпеки стає першорядним» [2, с. 187]. Важливість обізнаності про кібергігієну важко переоцінити. Оскільки цифрова сфера стає невід'ємною частиною нашого повсякденного життя – від особистого банківського обслуговування до глобальної торгівлі – потенційний вплив кіберзагроз виходить далеко за межі індивідуальних незручностей, створюючи значні ризики для нашої особистої конфіденційності [2, с. 93]. Звичайні громадяни дедалі більше потерпають від зростання кіберзлочинності, наприклад, під час придбання товарів чи банківських операцій у мережі Інтернет [1, с. 57]. Для протидії таким загрозам громадянам України необхідно дотримуватися правил цифрової грамотності, цифрового етикету, що охоплюється більш загальним поняттям «кібергігієна».

У Стратегії кібербезпеки України, затвердженій Указом Президента України від 15 березня 2016 року № 96, зазначається, що «швидко змінюваний цифровий світ потребує формування більш збалансованої та ефективної національної системи кібербезпеки, яка зможе гнучко адаптуватися до змін безпекового середовища, гарантуючи громадянам України безпечне функціонування національного сегмента кіберпростору, передбачивши нові можливості для цифровізації всіх сфер суспільного життя» [3].

Одним з недоліків реалізації попередньої Стратегії новою Стратегією кібербезпеки України визначено те, що розвиток цифрової грамотності здійснювався без чіткої програми, а кібернавчання проводились епізодично [3].

Результати аналізу наукових публікацій. Важливою для розуміння кібергігієни є розробка понятійного апарату у сфері кібербезпеки, яка стала предметом дослідження в роботах О. Баранова [4], В. Брижка, О. Довганя [5], А. Тарасюка, Т. Ткачука, В. Фурашева [6] та ін.

Сучасні підходи до дослідження кібербезпеки та кібергігієни в умовах цифрової трансформації суспільства висвітлювали у своїх роботах Ю. Білявська, Я. Шестак [1] та С. Федушко [7].

Організаційні аспекти впровадження цифрових технологій висвітлено такими вченими, як В. Круглов, В. Куйбіда, О. Карпенко, В. Наместнік [8]. Дослідження в цій галузі дозволяють з'ясувати наслідки використання цифрових пристроїв та програм для здоров'я населення та довкілля, щоб можна було розробити методи їх запобігання.

Актуальними з точки зору соціальної практики є дослідження кібергігієни в контексті запобігання вчиненню окремих кримінальних правопорушень [9]. Водночас сьогодні найбільш актуальним та затребуваним є дослідження кібергігієни як важливого чинника запобігання сучасним кіберзагрозам.

Проблема кібергігієни загострюється в умовах правового режиму воєнного стану, де люди розглядаються як об'єкти інформаційного впливу.

Метою статті є дослідження поняття кібергігієни, обґрунтування впровадження правил кібергігієни для запобігання сучасним кіберзагрозам.

Виклад основного матеріалу. Кібергігієна відіграє важливу роль у захисті від кіберзагроз як організацій, так і окремих осіб.

Кібергігієна стосується практик, які здійснюють окремі особи та організації для підтримки своєї цифрової безпеки та захисту від кіберзагроз. Це включає набір поведінкових правил, звичок і протоколів, які сприяють доброму кіберздоров'ю і знижують ризик кібератак [10].

Під терміном «кібергігієна» розуміється прищеплення і застосування навичок особистої інформаційної безпеки користувачами інформаційно-комунікаційної мережі Інтернет[1, с. 52]. Іншими словами, кібергігієна — це набір профілактичних заходів, яких кожен користувач має вживати для захисту своїх даних та пристроїв.

У більшості досліджень з цієї теми термін «кібергігієна» застосовується поряд з терміном «кібербезпека» [1; 7], тому співвідношення цих понять заслуговує на окрему увагу.

У буденному розумінні кібербезпека – це інформаційна безпека в умовах використання комп'ютерних систем та/або телекомунікаційних мереж [5, с. 61]. У найбільш широкому розумінні кібербезпека – це такий стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації [5, с. 61].

На нашу думку, кібергігієна є особливим інститутом кібербезпеки, призначення якого полягає у профілактиці і захисті від кіберзагроз на індивідуальному рівні або на рівні організації.

Слід погодитись із С. Федушко, яка вважає, що кібергігієна та кібербезпека – це два споріднені поняття у сфері цифрової безпеки, але вони стосуються різних аспектів захисту комп'ютерних систем та мереж від кіберзагроз [7, с. 212].

Аналогічно до звичайної гігієни кібергігієна спрямована на мінімізацію ризиків через дотримання певних правил, таких як: оновлення програмного забезпечення та операційних систем, регулярне резервне копіювання важливих даних, використання надійних паролів, уникнення підозрілих електронних листів і вебсайтів, регулярне резервне копіювання даних, впровадження брандмауерів та інших заходів безпеки. Належна кібергігієна допомагає запобігти кібератакам і мінімізувати шкоду, заподіяну в разі їх здійснення.

На думку С. Федушко, кібергігієна важлива для підтримки загальної цілісності комп'ютерних систем і мереж, а неналежні практики кібергігієни можуть послабити безпеку системи, роблячи її вразливою до атак [7, с. 211].

Дослідниця вважає, що приватні особи та організації повинні впроваджувати належні практики кібергігієни для того, 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 [7, с. 212]. Впроваджуючи належні практики кібергігієни, окремі особи та організації можуть мінімізувати ризик кібератак і зменшити тяжкість наслідків будь-яких успішних атак, які можуть статися [7, с. 211].

Серед ключових аспектів кібергігієни виділяють:

– захист особистих даних, оскільки більшість кібератак спрямована на отримання конфіденційної інформації, а дотримання правил кібергігієни допомагає мінімізувати ризики втрати даних;

– протидію фішингу. Інформування користувачів про методи шахраїв дозволяє зменшити кількість успішних атак;

– безпеку пристроїв, яка передбачає використання антивірусного програмного забезпечення та оновлення операційної системи, що суттєво підвищує захищеність таких пристроїв.

CERT-UA (спеціалізований структурний підрозділ Державного центру кіберзахисту

Державної служби спеціального зв'язку та захисту інформації України) пропонує основні правила кібергігієни: 1) будьте особливо обережними з відкриттям вкладень до електронної пошти від невідомих осіб. Під час роботи з поштою потрібно перевіряти розширення вкладених файлів та не відкривати файли навіть з безпечними розширеннями; 2) не переходьте за невідомими посиланнями та не завантажуйте файли, що мають потенційно небезпечне розширення (наприклад: .exe, .bin, .ini, .dll, .com, .sys, .bat, .js тощо) та навіть безпечне (наприклад: .docx, .zip, .pdf), адже можуть використовуватися вразливості, макроси та інші небезпеки; 3) проводьте роз'яснювальну роботу з підлеглими, що мають доступ до мережі Інтернет та працюють з поштовими агентами; 4) використовуйте ліцензійні/легалізовані операційні системи, інші програмні продукти, своєчасно й систематично їх оновлюйте; 5) користуйтеся антивірусним програмним забезпеченням з технологією евристичного аналізу; 6) здійснюйте регулярне резервне копіювання даних, зберігайте резервні копії на зовнішніх носіях інформації (SSD, HDD тощо) та налаштуйте функцію «відновлення системи»; 7) забороніть доступ до мережі Інтернет програмам, які потенційно можуть бути використані зловмисниками, якщо це не вплине на стабільність їх роботи [11].

Крім цього, правила кібергігієни передбачають:

– використання програмного міжмережевого екрану (брандмауера) та штатних засобів захисту від шкідливого програмного забезпечення;

– уникнення підключення флешок або зовнішніх дисків у комп'ютер, якщо немає довіри до їх джерела, оскільки сьогодні існують техніки зламування комп'ютера ще до відкриття файлу на флешці і задовго до його сканування антивірусом;

– уникнення зберігання автентифікаційних даних у легкодоступних місцях (наприклад, на робочому столі) з використанням для зберігання паролів спеціальних програмних засобів (наприклад, KeePass);

– уникнення використання Інтернет-банкінгу, електронних платіжних систем, введення автентифікаційних даних під час доступу до Інтернету через загальнодоступні (незахищені) безпроводові мережі (в кафе, барах, аеропортах та інших публічних місцях) [1, с. 56; 12].

Дотримання цих правил є вельми важливим для організацій, особливо в критично важливих галузях, таких як енергетика, логістика, медицина чи фінанси. Розробка внутрішніх політик інформаційної безпеки, проведення регулярних навчань для співробітників і впровадження сучасних технологій захисту є невід'ємною складовою частиною кібергігієни на рівні організацій.

Не менш важливими є освітні програми для населення у сфері кібергігієни.

Для досягнення ефективного рівня кібергігієни необхідне підвищення обізнаності населення. Зокрема, розробка освітніх програм для шкіл, університетів та професійних курсів сприятиме формуванню у суспільстві звички до безпечної роботи з цифровими технологіями. Як позитивний приклад можна відзначити освітній серіал координатора проєктів ОБСЄ в Україні у рамках проєкту «Посилення спроможностей українських державних органів у сфері кібергігієни та кібербезпеки», створений за підтримки урядів Німеччини та Сполученого Королівства у співпраці з Українською школою урядування. За даними світових досліджень, сьогодні є особливо високий попит на фахівців з кібербезпеки.

Проблема цифрової грамотності давно перебуває у фокусі держави.

Одним із напрямів державно-приватної взаємодії у сфері кібербезпеки Закон України «Про основні засади забезпечення кібербезпеки України» визначає підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки, реалізацію державних і громадських проєктів з підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту [13].

Ціль К.2 Стратегії кібербезпеки України звучить так: «Професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки» [13].

У цій частині Стратегія проголошує: «Для досягнення цілі К.2 в Україні буде проведено наукові дослідження у сфері кібербезпеки, реформовано систему під-

готовки та підвищення кваліфікації кадрів, а також розгорнуто навчальні програми, курси, тренінги з кібернавчання для всіх верств населення шляхом:

– забезпечення координації наукового співтовариства під час проведення наукових досліджень і розробок у сфері кібербезпеки та залучення його до заходів з реалізації державної політики у сфері кібербезпеки;

– визначення довгострокових напрямів проведення досліджень і розробок у сфері кібербезпеки, а також розроблення дієвої програми державної підтримки (на основі проєктного підходу) стратегічно важливих для кібербезпеки держави наукових установ і організацій, проведення наукових досліджень у цій сфері для потреб національної безпеки і оборони;

– забезпечення стимулювання досліджень і розробок у сфері кібербезпеки з урахуванням розвитку новітніх інформаційно-комунікаційних технологій, зокрема технологій хмарних та квантових обчислень, 5G-мереж, Інтернету речей, штучного інтелекту, з метою створення вітчизняних систем, платформ і продуктів у сфері кібербезпеки;

– удосконалення системи підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки;

– розроблення Загальнонаціональної програми кіберграмотності, спрямованої на підвищення рівня цифрової грамотності населення України, зокрема шляхом включення питань стосовно цифрових навичок, кіберобізнаності щодо сучасних кіберзагроз та їхній протидії до навчальних програм загальної середньої, професійної (професійно-технічної), фахової передвищої та вищої освіти» [13].

Завершення реалізації цих завдань було передбачене Планом заходів на 2023–2024 роки з реалізації Стратегії кібербезпеки України (затверджений розпорядженням Кабінету Міністрів України від 19 грудня 2023 р. № 1163).

Висновки. Одним з найбільш важливих чинників кіберзагроз є відсутність комплексної системи підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, чому сприяє низький рівень обізнаності суспільства щодо кіберзагроз та кіберзахисту. Ситуація ускладнюється активним використанням цифрових технологій у повсякденному житті, що зумовлює нові кіберзагрози.

Кібергігієна є одним із фундаментальних засобів запобігання кіберзагрозам як на особистому рівні, так і в масштабах організації та держави. Одним із ключових інструментів протидії кіберзагрозам є концепція кібергігієни – комплекс правил та практик, спрямованих на захист користувачів і організацій від кібератак.

Попри докорінну реформу системи підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки, стимулювання досліджень і розробок у сфері кібербезпеки з урахуванням появи нових кіберзагроз і викликів [13], проблемою залишається розвиток цифрової грамотності населення. Спроможність ефективно стримувати деструктивні дії в кіберпросторі, досягнення кіберстійкості на всіх рівнях та взаємодії всіх суб’єктів забезпечення кібербезпеки ґрунтується на довірі пересічних громадян, які мають дотримуватися правил кібергігієни. Цифрові навички, кіберобізнаність щодо сучасних кіберзагроз та протидія таким загрозам мають стати невід’ємними елементами освіти кожного громадянина України, як це передбачено Стратегією кібербезпеки України [13].

Соціологічні опитування керівників підприємств свідчать про те, що на підприємствах планують збільшити рівень витрат на кібербезпеку у подальшій роботі завдяки дотриманню правил кібергігієни, відповідальному ставленню до політики використання паролів та вчасному оновленню програмного забезпечення, вивченню слабкостей кіберзахисту й інвестуванню в найпростіші способи захисту від кіберзловмисників [1, с. 57].

Інвестиції у навчання, розробку політик та впровадження сучасних технологій дозволять суттєво зменшити ризики та забезпечити більш безпечне функціонування цифрового середовища. Україна має бути здатною забезпечити свій соціально-економічний розвиток у цифровому світі.

ЛІТЕРАТУРА:

1. Білявська Ю., Шестак Я. Кібербезпека та кібергігієна: нова ера цифрових технологій. *Товари і ринки*. 2022. № 3. С. 47–59. URL: http://nbuv.gov.ua/UJRN/tovary_2022_3_6 (дата звернення: 30.10.2024).

2. Кібербезпека в інформаційному суспільстві: інформаційно-аналітичний дайджест / відп. ред. О. Довгань ; упоряд. О. Довгань, Л. Литвинова, С. Дорогих ; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України» ; Національна бібліотека України ім. В.І. Вернадського. Київ, 2024. № 3 (березень). 339 с. URL: https://ippi.org.ua/sites/default/files/2024-3.pdf (дата звернення: 30.10.2024).

3. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серпня 2021 р. № 447. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 30.10.2024).

4. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека». *Правова інформатика.* 2014. № 2 (42). С. 54–62. URL: https://ippi.org.ua/sites/default/files/14boavpk.pdf (дата звернення: 30.10.2024).

5. Довгань О.Д., Тарасюк А.В., Ткачук Т.Ю. Кібербезпека «суспільства знань» : монографія. Київ ; Одеса : Фенікс, 2021. 173 с.

6. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право.* 2012. № 2. С. 162–169.

7. Федушко С. Сучасні підходи до дослідження кібербезпеки та кібергігієни в умовах цифрової трансформації суспільства. *Вісник Хмельницького національного університету.* 2023. № 3 (321). С. 210–213. URL: http://journals.khnu.km.ua/vestnik/wp-content/uploads/2023/07/vknu-ts-2023-n3321-210-213.pdf (дата звернення: 30.10.2024).

8. Куйбіда В.С., Карпенко О.В., Наместнік В.В. Цифрове врядування в Україні: базові дефініції понятійно-категорійного апарату. *Вісник Національної академії управління при Президентові України*. 2018. № 1. С. 5–10.

9. Медведенко Н.В. Кібербезпека та кібергігієна як засоби запобігання втручанням в діяльність захисника чи представника особи. *Юридичний науковий електронний журнал*. 2023. № 10. С. 394–398.

10. Кібергігієна. URL: https://www.vpnunlimited.com/ua/help/cybersecurity/cyber-hygiene (дата звернення: 30.10.2024).

11. Основні правила кібергігієни. CERT-UA. URL: https://cert.gov.ua/ (дата звернення: 30.10.2024).

12. Кібергігієна. Північне міжрегіональне головне управління Державної служби України з питань безпечності харчових продуктів та захисту споживачів на державному кордоні. URL: https://nir.gov.ua/kibergigiyena/ (дата звернення: 30.10.2024).

13. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовтня 2017 р. № 2163. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 30.10.2024).