УДК 008.2
DOI: 10.31673/2412-9070.2021.031216

Я. А. ДЕРКАЧЕНКО, аспірант;
Т. М. ДЗЮБА, канд. техн. наук, доцент,
Державний університет телекомунікацій, Київ

ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ УКРАЇНИ ЗА СУЧАСНИХ УМОВ: ЦИФРОВІ НАВИЧКИ ТА КОМПЕТЕНТНОСТІ

Розглянуто роль цифрових навичок у цифровій економіці як один з елементів системи кібербезпеки України. Визначено поняття «цифрові навички». Проаналізовано основні нормативно-правові документи системи національної безпеки. Запропоновано власне визначення поняття «переосмислення» та поділено його на «переосмислення продукту» і «персональне переосмислення». Виокремлено елементи для формування цифрової компетенції з інформаційної та кібербезпеки. Розкрито тему нових спеціалізацій кібербезпеки.

Ключові слова: цифрова економіка; цифрові навички; цифрові компетенції; кібербезпека; спеціалізації кібербезпеки; переосмислення.

ВСТУП

Постановка проблеми. У Стратегії національної безпеки України [1] визначено три основні засади забезпечення національної безпеки: стримування, тобто розвиток оборонних і безпекових спроможностей для унеможливлення збройної агресії проти України, стійкість, тобто здатність суспільства та держави швидко адаптуватися до змін безпекового середовища й підтримувати стале функціонування, зокрема мінімізацією зовнішніх і внутрішніх уразливостей, та взаємодія, тобто розвиток стратегічних відносин із ключовими іноземними партнерами, насамперед з Європейським Союзом і НАТО та їх державами-членами, Сполученими Штатами Америки, прагматичне співробітництво з іншими державами та міжнародними організаціями на основі національних інтересів України. Вочевидь, що засади стримування та взаємодії практично повністю стосуються відповідної діяльності державних установ, а також суб'єктів Сектору безпеки і оборони України. Проте реалізація засади «стійкість» залежить фактично від усіх громадян України.

Кібербезпека є невід'ємною складовою системи національної безпеки України. А отже, від кожного громадянина залежить стан кіберстійкості нашої держави. Особливої важливості це набуває за умов переходу України від традиційної економіки до цифрової, тобто економіки, яка базується на цифрових комп'ютерних технологіях та інформаційно-комунікативних технологіях [2]. Основою як кіберстійкості, так і готовності до впровадження механізмів цифрової економіки є формування необхідних цифрових навичок та компетенцій наших громадян.

Аналіз останніх досліджень і публікацій. Опосередковано досліджували цифрові навички такі українські вчені, як І. В. Діордіца, В. А. Ліпкан, І. В. Арістова, І. М. Сопілко, Н. С Журавська, О. В. Струтинська, С. В. Легомінова та ін. Проте, незважаючи на наявність базових наукових напрацювань, їх основний акцент було зосереджено на розвитку та становленні інформаційного суспільства, інформаційної культури, кібербезпекової політики, напрямків підготовки фахівців із кібербезпеки. Цифрові навички та їх роль у системі кібербезпеки сьогодні мало вивчені. Відсутність ґрунтовного дослідження зумовлює потребу в більш детальному розкритті цієї теми.

Мета статті полягає в дослідженні процесу формування цифрових навичок громадян та їх ролі в національній системі кібербезпеки. Крім того, проведене дослідження дало змогу сформувати певні висновки щодо тих галузей діяльності, які вже сьогодні стають обов'язковими для цифрової економіки.

ОСНОВНА ЧАСТИНА

Згідно з проведеним дослідженням Всесвітнього економічного форуму більш як 50% населення Землі щодня перебувають у мережі «Інтернет». Щодня майже один мільйон людей приєднується до інтернету. Дві третини людства мають мобільний пристрій [3].

Технології цифрової економіки здатні розв'язувати проблему взаємовідносин громадянського суспільства, бізнесу і держави, приносячи істотні економічні та соціальні вигоди. Технології Розумного міста та дому, Інтернету речей, масової цифровізації державних послуг, реалізація проєкту «Країна в смартфоні» мають величезний потенціал для покращення життя людини та підвищення її безпеки існування.

Водночас треба розуміти, що поява нових переваг породжує нові ризики для соціотехнічних систем цифрової економіки, тобто систем, складовою яких є людина-оператор, знання, уміння, настрої, ціннісні переваги й ставлення до виконуваних обов'язків, які виявляються у взаємодії з технічними пристроями [4].

Кіберпростір виступає як основа для обміну інформацією та даними соціотехнічних систем, що й зумовлює його розгляд як середовища взаємозв'язаних технічних ризиків. Відповідно до міжнародних стандартів у сфері інформаційної та кібернетичної безпеки до таких технічних ризиків належать: порушення цілісності та доступності інформаційно-комунікаційної інфраструктури, несприятливі технологічні досягнення, шахрайство та крадіжка даних, кібератаки. З погляду ймовірності та впливу серед зазначених технічних ризиків експерти дослідження «The Future of Jobs Report 2020» [3] акцентують свою увагу на десятьох глобальних ризиках, до яких входять кібератаки та шахрайства/крадіжки даних.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» об'єктами кібербезпеки та кіберзахисту є такі [5]:

♦ конституційні права та свободи людини і громадян;

♦ національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;

♦ суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища.

Важливим кроком у формуванні першої в історії нашої держави дорожньої карти з кібербезпеки та кіберзахисту стало затвердження «Стратегії кібербезпеки України» 27-го січня 2016 року [6]. Одним із пріоритетних напрямків забезпечення кібербезпеки України в Стратегії визначено формування цифрових навичок, а саме: підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексні знання, навички і здібності, необхідні для підтримання цілей кібербезпеки, упровадження державних і громадських проєктів підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту.

Також варто виокремити розроблення «Проєкту Стратегії кібербезпеки України на 2021-2025 роки» [7]. Цей стратегічний документ розроблено Національним координаційним центром кібербезпеки при Раді національної безпеки і оборони України в рамках нової Стратегії національної безпеки України. Метою Стратегії визначено створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства, держави. Документ ґрунтується на засадах стримування, кіберстійкості та взаємодії.

Для набуття кіберстійкості національною системою кібербезпеки до 2026 року потрібно досягти таких стратегічних цілей:

♦ посилення національної кіберготовності та кіберзахисту;

♦ забезпечення надійності та безпеки цифрових послуг із моменту створення та протягом усього їхнього життєвого циклу;

♦ професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки.

Проведений нами аналіз нормативно-правової бази дав змогу переконатися, що цифрові навички та компетенції населення є одним із стратегічних елементів системи кібербезпеки України в межах переходу до цифрової економіки.

Окремо варто закцентувати увагу на відсутності уніфікованої дефініції «цифрових навичок». Серед як науковців, так і законотворців відбувається розмиття рамок цього терміна.

На думку авторів, ***цифрові навички*** — комплекс навичок, що передбачають впевнене, критичне та відповідальне використання інформаційно-комунікаційних технологій для навчання, роботи й життя в цифровому суспільстві.

До цифрових навичок належать:

- інформаційна грамотність;
- медіаграмотність;
- опрацювання даних із використанням цифрових технологій;
- комунікація та співпраця з використанням цифрових технологій;
- уміння створювати цифровий контент, зокрема програмування;
- обізнаність у питаннях інтелектуальної власності;
- уміння вирішувати проблеми з використанням цифрових технологій;
- уміння критично мислити;
- інформаційна та кібербезпека.

Далі на підставі аналізу сучасних досліджень і публікацій розглянемо детальніше деякі з цифрових навичок.

Переосмислення

Сучасному нестабільному світові, відповідно до теорії VUCA, характерні такі властивості: мінливість (volatile), невизначеність (uncertain), складність (complex) та неоднозначність (ambiguous).

Згідно з дослідженням Reinvention Academy, щоб залишатися на плаву і бути конкурентоспроможним на ринку праці в сучасному світі, ми маємо постійно переосмислювати себе чи продукт компанії з періодичністю кожні 3,5 роки [8].

Термін «переосмислення» в українській мові є новим та мало дослідженим. У словнику української мови СУМ-11 у поняття «переосмислити» вкладається таке значення: осмислювати по-своєму або по-іншому [9].

В англійській мові процес створення чогось нового, що базується на чомусь, що вже існує, характеризується терміном «reinvention».

Отже, пропонуємо в українській мові використовувати слово «переосмислення» для позначення процесу створення якісно нового продукту, який ґрунтується на наявному продукті, та поділяти на власне «персональне переосмислення» і «переосмислення продукту».

Переосмислення продукту — комплекс заходів, які допомагають компанії стати менш уразливою перед різноманітними викликами і досягти значно кращих результатів [8].

Деннінг С. у своїй статті Forbes стверджує: «Півстоліття тому життєвий цикл компаній, що входив у рейтинг Fortune 500, становив майже 75 років. Сьогодні ж цей термін становить менш як 15 років і продовжує скорочуватися» [10].

Активна глобалізація та доступна онлайн-освіта сприяла появі абсолютно нових винаходів і стартапів. Попри значну кількість успішно запущених стартапів, лише третина з них зможе проіснувати до 10-ти років. Отже, сучасні реалії створюють підвищений попит до процесу «переосмислення».

Персональне переосмислення — процес передбачення, проєктування і впровадження внутрішніх змін: здобуття нових навичок до того, як настануть зовнішні зміни.

Вимирання професій через автоматизацію робочих бізнес-процесів разом з іншими проблемами стрімко мінливого ринку праці вже сьогодні змушують суспільство нервувати і замислюватися про зміну професій.

Як зазначив американський футуролог Тоффлер Е., один з авторів концепції «Інформаційної цивілізації»: «Безграмотними в XXI столітті будуть не ті, хто не вміє читати і писати, а ті, хто не вміє вчитися, розучуватися і перенавчатися».

Військовий історик та філософ Харарі Ю. Н. впевнений, що більшість навичок, які нині здобувають у школах та закладах вищої освіти, швидко стають нерелевантними, а професії втрачають конкурентоспроможність на ринку праці: «Варто забути про програмування, найкраща навичка для навчання дітей — це переосмислення».

Ньюмейер М. у своїй книзі «Метанавички. П'ять талантів в епоху роботизації» виокремлює здатність до навчання, здатність набувати нових навичок як одну з п'яти навичок, необхідних людям для досягнення успіху в епоху четвертої промислової революції.

Цифрові навички та компетенції з інформаційної та кібербезпеки

Окремо особливу увагу слід приділити низькому рівню навичок з інформаційної та кібербезпеки населення України, зокрема пересічних користувачів електронних послуг, що закладає підґрунтя для формування недовіри до держави та зберігає наявні ризики та загрози в кіберпросторі.

На нашу думку, до основних таких навичок належать:

- усвідомлення власної ролі та обов'язків у системі кібербезпеки України;
- уміння класифікувати персональну інформацію відповідно до власної цінності;
- налаштування захисту облікових записів;
- створення та безпечне зберігання стійких паролів;
- налаштування безпеки мобільних пристроїв;
- робота з мобільними банками та електронні фінансові операції;
- поінформованість щодо процедури реагування на підозру в компроментації;
- поінформованість щодо процедури «Як швидко? За допомогою якого каналу? До якого суб'єкта системи забезпечення кібербезпеки України?» звертатися в разі інциденту інформаційної безпеки чи підозри у витоку персональних даних;
- переосмислення власних професійний навичок.

Відставання сфери освіти від процесів зародження та формування нових потреб бізнес-середовища створює брак спеціалістів на ринку праці.

У Постанові КМУ № 266 «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» від 29.05.2015 року щодо інформаційної та кібербезпеки у ВНЗ виокремлено лише одну спеціальність 125. Кібербезпека, відповідно до якої відбувається підготовка здобувачів вищої освіти [11].

Назріває потреба стосовно внесення змін у перелік галузей знань і спеціальностей, розширення шифру галузі та коду спеціалізації. З огляду на міжнародні стандарти, регламенти, методології та практики інформаційної та кібербезпеки ISO 27001/27002, PCI DSS, NIST, GDPR, Owasp, на нашу думку, відбувається чітке розгалуження сфери кібербезпеки, що поступово призводить до зникнення наявних спеціалізацій. Очікуваним результатом цієї тенденції є поява нових спеціалізацій у сфері інформаційної та кібербезпеки щодо вирішення проблем ринку праці сьогодення та майбутнього.

До таких спеціалізацій варто віднести:

♦ ***аудитор стратегічної (зокрема й інформаційної та кібернетичної) інфраструктури***. У процесі формування та реалізації державної політики кожна держава імплементує національні стандарти інформаційної та кібернетичної безпеки для об'єктів стратегічної інфраструктури заради реалізації національних інтересів. Аудитор стратегічної інфраструктури, маючи відповідну компетенцію, отримуючи унормований чинним законодавством належний доступ, здійснюватиме перевірку відповідності, ефективності системи кібербезпеки об'єктів стратегічної інфраструктури

задля виконання ними життєво важливих функцій і надання життєво важливих послуг, збереження стійкості за умови впливу чинників різної природи;

• ***фахівець із телекомунікаційної безпеки***. Поступовий перехід та розгортання мережі 5G продовжує зберігати недоліки захищеності протоколів, використовуваних у мережах 2G, 3G і 4G. Основними споживачами послуг 5G зв'язку є Інтернет речей, які поступово починають забезпечувати важливі функції Розумного міста, елементів Розумного дому, промислової та стратегічної інфраструктури в цілому.

Через свою особливість та специфіку сектор телекомунікаційної безпеки суттєво різниться від звичайної мережної безпеки. Основною задачею фахівця з телекомунікаційної безпеки має виступати покращення рівня кібербезпеки телекомунікаційних мереж мобільного зв'язку;

• ***кіберстраховий агент***. Основним завданням кіберстрахування є захист від кібер-ризиків за допомогою передавання частини ризиків порушення інформаційної безпеки на страхову компанію.

Такий вид страхування забезпечує фінансовий механізм відновлення після значних збитків, допомагаючи компанії повернутися до нормального функціонування зі збереженням стійкості в результаті перерви в діяльності.

Кіберстраховий агент здійснюватиме свою діяльність у повному супроводженні життєвого циклу страхового продукту;

• ***фахівець із кібербезпеки Інтернету речей***. Аналітичні компанії прогнозують, що до 2023 року ринок продажу розумних пристроїв досягне 1,46 млрд одиниць на рік.

Фахівець із кібербезпеки вбудованих систем зосереджуватиметься на захисті Інтернету речей від загроз шпигунства, отримання фінансової вигоди та завдання шкоди репутації власникам;

• ***менеджер із безпеки цифрової репутації***. Сучасні реалії зумовлюють ототожнення інформації до цінного активу. Використовуючи власно створені мережі шахрайських інтернет-ресурсів, злодії здійснюють кібертеторизм публічних осіб та відомих компаній через публікацію низки статей негативного вмісту. Як результат, пошукові мережі за ключовими ідентифікаторами особи демонструють негативний імідж об'єкта, спричинюючи взаємозалежні негативні наслідки під час перевірки цифрової репутації.

Менеджер із безпеки цифрової репутації здійснюватиме дії, спрямовані на виявлення, попередження, запобігання та коригування негативного цифрового відбитку як окремо взятої особи, так і репутації компанії;

• ***фахівець із кібербезпеки штучного інтелекту***. Здійснений нами аналіз дослідження, яке було виконано в Capgemini Research Institute 2019 року, дав можливість встановити той факт, що майже 69% компаній вважають, що в майбутньому штучний інтелект стане невід'ємним елементом системи кібербезпеки. Якщо в 2019 році тільки кожна п'ята компанія використовувала вирішення, пов'язані зі штучним інтелектом, то в 2020 році їх кількість сягнула вже майже дві третини.

Попит на вирішення на основі штучного інтелекту породжує потребу у фахівцях із кібербезпеки штучного інтелекту.

Висновки

Проведений нами аналіз дав змогу встановити роль цифрових навичок у цифровій економіці та системі кібербезпеки України. Пріоритетність формування цифрових навичок громадян доведено не тільки в дослідженнях учених-теоретиків, а й в нормативних актах та законах України. Мінливість, невизначеність, складність та неоднозначність сучасного світу зумовлюють важливість використання практики переосмислення як персонального, так і переосмислення продукту компанії.

Колишні компетенції та спеціалізації втрачають свою актуальність через формування нового бізнес-середовища. Реформування системи освіти потребує, щоб Міністерство освіти та науки України невідкладно внесло зміни в освітньо-кваліфікаційну характеристику, професійні програми та перелік галузей знань і спеціальностей, за якими здійснюється підготовка майбутніх спеціалістів з інформаційної та кібербезпеки майбутнього.

Список використаної літератури

1. ***Стратегія*** *національної безпеки України, затверджена Указом Президента України від 14 вересня 2020 року № 392/2020 [Електронний ресурс]. URL:*

https://www.president.gov.ua/documents/3922020-35037;

2. ***Пищуліна О.*** *Цифрова економіка: тренди, ризики та соціальні детермінанти. Центр Разумкова, 2020.*

3. ***Report*** *The Future of Jobs 2020 World Economic Forum [Електронний ресурс]. URL:*

http://www3.weforum.org/docs/WEF_Future_of_Jobs_2020.pdf

4. ***Інформаційна*** *та кібербезпека: соціотехнічний аспект / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа [Електронний ресурс]. URL:*

http://www.dut.edu.ua/uploads/p_303_79299367.pdf

5. ***Закон*** *України «Про основні засади забезпечення кібербезпеки України» від 24.10.2020 [Електронний ресурс]. URL:*

https://zakon.rada.gov.ua/laws/show/2163-19#Text

6. ***Стратегія*** *кібербезпеки України від 15.03.2016 [Електронний ресурс]. URL:*

https://zakon.rada.gov.ua/laws/show/96/2016#Text

7. ***Стратегія*** *кібербезпеки України (2021 – 2025 роки) [Електронний ресурс]. URL:*

https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf

8. ***Zhexembayeva N.*** *Titanic Syndrome Titanic syndrome: the living book [Електронний ресурс]. URL:*

https://chiefreinventionofficer.com/titanic-syndrome

9. ***Словник*** *української мови: в 11 т. Т. 6, 1975. С. 242 [Електронний ресурс]. URL:*

http://sum.in.ua/s/pereosmysljuvaty

10. ***Steve Denning.*** *Peggy Noonan On Steve Jobs And Why Big Companies Die [Електронний ресурс]. URL:*

https://www.forbes.com/sites/stevedenning/2011/11/19/peggy-noonan-on-steve-jobs-and-why-big-companies-die/?sh=233fabe6cc3a

11. ***Про затвердження*** *переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти: Постанова Кабінету Міністрів України від 29.04.2015 №266 [Електронний ресурс]. URL:*

https://npu.edu.ua/images/file/Viddil_licen/2016/post_266.pdf

Я. А. Деркаченко, Т. М. Дзюба

ОБЕСПЕЧЕНИЕ КИБЕРСТОЙКОСТИ УКРАИНЫ В СОВРЕМЕННЫХ УСЛОВИЯХ: ЦИФРОВЫЕ НАВЫКИ И КОМПЕТЕНТНОСТИ

Рассмотрена роль цифровых навыков в цифровой экономике как одного из элементов системы кибербезопасности Украины. Дано определение понятия цифровые навыки. Предложено собственное определение понятия «переосмысление». Выделены элементы для формирования цифровых компетенций по информационной и кибербезопасности. Раскрыта тема новых специализаций кибербезопасности.

Ключевые слова: цифровая экономика; цифровые навыки; цифровые компетенции; кибербезопасность; специализации кибербезопасности; переосмысление.

Ya. A. Derkachenko, T. M. Dzyuba

ENSURING THE CYBER RESISTANCE OF UKRAINE IN MODERN CONDITIONS: DIGITAL SKILLS AND COMPETENCIES

This article reviews the role of digital skills in the digital economy as one of the elements of Ukraine's cybersecurity systems. The author examines the process of formation of digital skills of citizens and defines the concept of «digital skills». The author has named the base list of digital skills. View cyberspace as an environment for the exchange of information and data of socio-technical systems. The technical risks that are characteristic of cyberspace have been called: violation of the integrity and accessibility of information and communication infrastructure, adverse technological advances, fraud and data theft, cyber-attacks.

The author analyzes the main legal documents of the national security system. Highlights the low level of skills in information and cyber security in Ukraine, which forms the basis for the formation of non-admission to the state and the storage of other risks and threats in cyberspace. Considers the strategic goals of the national cybersecurity system of Ukraine. The emphasis is on the characteristic power properties of instability in the modern world: variability, uncertainty, complexity, and ambiguity. Offers its definition of «rethinking» and extends it to «product rethinking» and «personal rethinking». Separates elements for the formation of digital competencies in information and cybersecurity. Explains the topic of new specialized cybersecurity and lists them: auditor of strategic (including information and cyber) infrastructure, telecommunications security specialist, cyber insurance agent, Internet of Things cybersecurity specialist, digital reputation security manager, Specialist in cybersecurity of Artificial intelligence.

Keywords: digital economy; digital navigation; digital competencies; cybersecurity; cybersecurity specialization; rethinking.