Міщенко Володимир Іванович
доктор економічних наук, професор,
завідувач сектору цифрової економіки,
Державна установа «Інститут економіки та прогнозування
Національної академії наук України»;

Науменкова Світлана Валентинівна
доктор економічних наук, професор,
професор кафедри фінансів,
Київський національний університет
імені Тараса Шевченка

DOI: https://doi.org/10.36059/978-966-397-253-4-5

НАПРЯМИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ЕКОНОМІКИ УКРАЇНИ В ПЕРІОД ПОВОЄННОГО ВІДНОВЛЕННЯ

Ключовими напрямами поглиблення цифрових трансформацій в умовах повоєнного відновлення та реструктуризації економіки України повинні бути: розвиток на новій технічній та технологічній основі ключових елементів загальнодержавної цифрової інфраструктури; вдосконалення роботи з відкритими даними, головною метою якої повинно бути забезпечення ефективної конвертації даних в інші види ресурсів (перш за все, в ті, які становлять суспільний інтерес); посилення кібербезпеки та розроблення нових механізмів управління кіберстійкістю та кіберризиками; широке впровадження нових інформаційно-комунікаційних технологій в системі освіти та охорони здоров'я, зменшення рівня «цифрового розриву» та інші [1, с. 198; 2, с. 425; 3, с. 38; 4, с. 187; 5, с. 154].

Вдосконалення загальнодержавної цифрової інфраструктури повинно передбачати, перш за все, відновлення роботи щодо впровадження в Україні нової технології зв'язку 5G шляхом використання відповідних технічних і технологічних рішень, організації підтримки та контролю угод між операторами зв'язку про спільне використання інфраструктури з метою зниження витрат на розгортання та використання мережі 5G [6, с. 77].

З метою посилення механізмів роботи з відкритими даними та ефективного функціонування Єдиного державного веб-порталу відкритих даних нагальними питаннями є: забезпечення переходу на використання стандарту DCAT-AP для порталів відкритих даних у версії v2.1.0; збільшення обсягів надання інформації в режимі реального часу та розширення посилань на різні джерела походження та постачальників даних; реалізація програм перетворення даних в альтернативні формати та оцінки профілів користувачів і їхніх потреб; розширення переліку державних картографічних і природних даних; включення до веб-порталу даних про якість води та повітря; розроблення та затвердження системи показників для вимірювання, моніторингу та оцінки впливу відкритих даних на економічні та соціальні процеси в країні [7, с. 70; 8, с. 137; 9, с. 39].

На окрему увагу заслуговують питання вдосконалення регулювання доступу, поширення та використання конфіденційних даних, які стосуються, перш за все, актуальних аспектів забезпечення національної безпеки та оборони, кібербезпеки, життєдіяльності громадян, комерційної таємниці, інтелектуальної власності тощо. Для цього доцільним є розроблення та затвердження переліку «даних, які мають суспільний інтерес», а також чітке визначення законодавчих положень, які повинні забезпечувати обов’язкове надання приватними підприємствами таких даних органам державної влади [9, с. 42; 10, с. 158].

З метою посилення технічних аспектів кібербезпеки доцільним є включення відповідних інструментів її підтримки в технологічні та технічні можливості програмного забезпечення, зокрема, захист від шкідливого коду в кінцевому обладнанні на всіх етапах його створення та використання шляхом стандартизації та кодифікації контрольно-інженерних і технологічних процесів, а також проведення специфікації програмного забезпечення з деталізацією всіх його структурних складових (наприклад, компоненти з відкритим вихідним кодом, компоненти в кодовій базі, інструменти сканування коду, галузеві стандарти та вимоги тощо).

Для підвищення рівня безпеки об’єктів і продуктів Інтернету речей необхідно забезпечити промислове маркування нових пристроїв та організувати систему постійного моніторингу безпеки вже підключених пристроїв. Крім того, розробники продуктів (об’єктів) Інтернету речей повинні обов’язково надавати користувачам відповідну інформацію щодо специфікації такого програмного забезпечення.

З метою посилення інституційної спроможності органів державної влади надійно та ефективно підтримувати національну екосистему кібербезпеки та кіберстійкості необхідно законодавчо забезпечити комплексну реалізацію таких заходів:

– визначити терміни, обсяг, зміст, умови, форми та засоби збереження конфіденційності всієї інформації про кібкрінциденти, яку обов’язково повинні надавати об’єкти критичної інфраструктури та існуючі публічні реєстри Державному центру кіберзахисту України;

– розробити та затвердити перелік об’єктів критичної інфраструктури та перелік об’єктів критичної цифрової (інформаційної) інфраструктури, а також передбачити дієві механізми для його періодичного оновлення та актуалізації;

– розробити механізми взаємодії Державного центру кіберзахисту України, об’єктів критичної інфраструктури та критичної цифрової інфраструктури, чітко визначивши їх права, обов’язки та відповідальність у процесі взаємодії з питань кіберзахисту та підтримки кіберстійкості;

– зобов’язати акціонерні товариства, які є власниками об’єктів критичної інфраструктури, розкривати чітко визначений обсяг інформації про кібкрінциденти своїм інвесторам та акціонерам;

– створити при Державному центрі кіберзахисту України репозитарій інформації про кіберінциденти, визначити рівні доступу до його даних та умови використання інформації суб’єктами господарювання;

– розробити для підприємств, організацій та установ методичні рекомендації щодо управління кібербезпекою та забезпечення кіберстійкості, які б містили стандартні архітектури таких процесів;

механізми організації, методи вимірювання та оцінки рівня кіберзахисту; вимоги до компетенцій ключового персоналу та професійних сертифікацій осіб, які відповідають за виявлення та попередження кіберінцидентів; механізми управління вразливостями та реагування на кібератаки, а також порядок звітування про стан кібербезпеки та кіберстійкості підприємств, організацій та установ.

Крім того, в контексті реалізації механізмів забезпечення кіберстійкості галузевим регуляторам ринку доцільно запровадити на підприємствах, в організаціях і установах обов'язкове розроблення та реалізацію комплексних систем забезпечення кіберстійкості та управління кіберризиками. Такі системи повинні ґрунтуватися на реалізації стратегій раннього виявлення кіберзагроз і розробленні адекватних політик кібербезпеки, передбачати мінімізацію негативного впливу від реалізації кібератак та інших кіберзагроз, забезпечення цілісності, доступності та конфіденційності даних, які обробляються, зберігаються та передаються за допомогою телекомунікаційних систем, а також можливість відновлення діяльності до умов функціонування у стандартному режимі. Принципово важливим елементом такої системи повинно бути визначення мінімально допустимого (базового) рівня кібербезпеки (кіберстійкості) підприємства.

Важливим напрямом посилення цифрової трансформації економіки України в період повоєнного відновлення повинно бути всебічне стимулювання впровадження нових інформаційно-комунікаційних технологій в системі освіти, для чого, зокрема, необхідно:

– розробити національні стандарти акредитації та сертифікації вчителів з урахуванням вимог до їх цифрової кваліфікації та навичок безпечного й відповідального використання Інтернету;

– запровадити в старших класах загальноосвітніх шкіл курс з інформаційно-комунікаційних технологій з проведенням сертифікації цифрових навичок і компетенцій учнів;

– врахувати в програмах університетів вивчення основ штучного інтелекту, кібербезпеки, великих даних, квантових та інших

цифрових технологій з метою синхронізації освітніх стандартів вітчизняних університетів з університетами Європейського Союзу, а також сприяти розвитку R&D, наукових парків та IT-освіти.

Список використаної літератури:

1. Mishchenko S., Naumenkova S., Mishchenko V., Dorofeiev D. Innovation risk management in financial institutions. *Investment Management and Financial Innovations*. 2021. Vol. 18. Is. 1. P. 190–202.
2. Міщенко В. І., Міщенко С. В. Удосконалення дії каналів трансмісійного механізму грошово-кредитної політики в Україні в умовах переходу до таргетування інфляції. *Актуальні проблеми економіки*. 2015. № 1. С. 421–428.
3. Іванов В. В., Науменкова С. В. Економіко-правові колізії дослідження фінансових ринків. *Вісник Київського національного університету імені Тараса Шевченка. Економіка*. 2013. № 12 (153). С. 35–41.
4. Mishchenko, V., Naumenkova S., Grytsenko A., Mishchenko S. Operational Risk Management of Using Electronic and Mobile Money. *Banks and Bank Systems.* 2022. Vol. 17. Is. 3. P. 142–157. DOI: http://dx.doi.org/10.21511/bbs.17(3).2022.12.
5. Міщенко В. І., Науменкова С. В. Поняття системного ризику та підходи до визначення системно значущих банків. *Соціально-економічні проблеми сучасного періоду України*. 2014. Т. 1. № 105. С. 186–189.
6. Міщенко В. І. Стратегічне управління процесами цифрової трансформації економіки. *Економіка України*. 2022. № 1. С. 67–81. DOI: https://doi.org/10.15407/economyukr.2022.01.067.
7. Науменкова С. В., Мищенко С. В. Регулирование денежного обращения на основе использования методов и инструментов денежно-кредитной политики. *Вісник Київського національного університету імені Тараса Шевченка*. 2013. № 6 (147). С. 66–72.
8. Ivanov V. V., Lvova N. A., Pokrovskaia N. V., Naumenkova S. V. Determinants of tax incentives for investment activity of enterprises. *Journal of Tax Reform*. 2018. Vol. 4. Is. 2. P. 125–141.
9. Міщенко В. І. Механізми регулювання обміну даними. *Причорноморські економічні студії*. 2022. № 75. С. 37–45. DOI: https://doi.org/10.32843/bses.75-6.
10. Bukovinsky S. A. et al. The Banking System of Ukraine: Towards European Integration. Kyiv : National Bank of Ukraine, 2015. 496 p.