УДК 004.9:316.4

ЦИФРОВИЙ ВИМІР КУЛЬТУРИ ОСОБИСТОЇ БЕЗПЕКИ

Нікітенко В. О.
доктор філософських наук, професор,
Таврійський державний агротехнологічний університет імені Дмитра Моторного,
м. Запоріжжя, Україна.
ORCID: https://orcid.org/0000-0001-9588-7836

Нестеров О. С.
старший викладач кафедри фізичного виховання і спорту
Таврійський державний агротехнологічний університет імені Дмитра Моторного,
м. Запоріжжя, Україна
ORCID: https://orcid.org/0000-0001-5016-6314

Цифровізація економіки, освіти та повсякденного життя створює для молоді одночасно безпрецедентні можливості й нові конфігурації ризиків, пов'язаних із використанням даних, онлайн-ідентичності, фінансових інструментів і цифрових платформ. В умовах війни проти України ці ризики посилюються: від цілеспрямованих інформаційних операцій і кібератак до зростання фінансового шахрайства, онлайн-насильства та маніпуляцій, спрямованих на вразливі групи молоді. У такій ситуації культура особистої безпеки набуває виразного цифрового виміру, у межах якого центральними стають питання захисту персональних даних, цифрової гігієни, протидії дезінформації, безпечного використання фінансових і платформених сервісів, а також збереження психологічної стійкості в цифровому середовищі [1].

Університети, будучи ключовими акторами вищої освіти та цифрової трансформації, дедалі більше виконують роль інституційних посередників між цифровою економікою та молоддю. З одного боку, саме вони готують майбутніх фахівців для секторів IT, фінансових технологій, медіа, креативних індустрій. З іншого – університети стають майданчиками, де формується цифрова культура студентства: норми використання інформаційних ресурсів, ставлення до конфіденційності, моделі онлайн-спілкування, готовність протидіяти кіберризикам. У цьому контексті цифровий вимір культури особистої безпеки має бути невід'ємним компонентом сталого розвитку вищої освіти, що об'єднує технологічні, етичні, правові та психосоціальні аспекти [2].

Цифрова культура безпеки молоді розуміється як інтегрована компетентнісна система, що включає:

а) здатність критично оцінювати цифрові ризики (витік даних, шахрайство, онлайн-насильство, маніпуляції);

б) навички захисту власної цифрової ідентичності та персональних даних;

в) відповідальне використання платформ, соціальних мереж, сервісів електронної комерції та онлайн-банкінгу;

г) розуміння правових рамок (цифрові права, GDPR-подібні норми, академічна доброчесність);

д) елементи психологічної стійкості до інформаційного перевантаження, токсичного контенту й хейту.

Таким чином, цифровий вимір особистої безпеки виходить далеко за межі «технічної» кібербезпеки і включає ширший соціально-економічний та етичний контекст. З огляду на Цілі сталого розвитку ООН, цифровий вимір культури особистої безпеки безпосередньо пов'язаний з ЦСР 4 «Якісна освіта», ЦСР 8 «Гідна праця та економічне зростання», ЦСР 9 «Інновації та інфраструктура» та ЦСР 16 «Мир, справедливість та сильні інституції». Формування у молоді стійких компетентностей цифрової безпеки дає змогу зменшувати вразливість до економічних і соціальних ризиків, пов'язаних із шахрайством, експлуатацією,

порушенням прав і свобод, а також підтримує розвиток інклюзивної цифрової економіки, де інновації не підривають базові стандарти прав людини й гідності. Університети в цьому контексті виступають не лише «постачальниками кадрів» для цифрової економіки, а й регуляторами цифрової етики – через освітні програми, внутрішні політики, кодекси поведінки в онлайн-середовищі [3].

Змістовно цифровий компонент безпеки включає кілька ключових блоків: цифрову гігієну та базову кібербезпеку (робота з паролями, двофакторною автентифікацією, перевіркою джерел інформації), захист персональних даних і конфіденційності, протидію онлайн-насильству (кібербулінг, домагання, мова ворожнечі), безпечне використання фінансових сервісів (онлайн-банкінг, платіжні сервіси, інвестиційні платформи), а також елементи цифрового добробуту (баланс онлайн/офлайн, управління часом, критичне ставлення до алгоритмічно сформованих стрічок).

Структура цифрового виміру культури особистої безпеки молоді в університетському середовищі, доцільно виділити основні блоки компетентностей, типові ризики та орієнтири освітньо-інституційних інтервенцій (табл. 1).

Таблиця 1

Структура цифрового виміру культури особистої безпеки молоді в університетському середовищі в Україні

Блок цифрової безпеки	Типові ризики для молоді	Цільові компетентності та інституційні відповіді
Захист персональних даних і цифрової ідентичності	Несанкціонований доступ до акаунтів, крадіжка особистих даних, неусвідомлене погодження з інвазивними політиками конфіденційності	Здатність налаштовувати приватність, критично читати умови використання сервісів; ухвалення університетських політик захисту даних та інформування студентів про їхні цифрові права
Протидія онлайн-насильству та дезінформації	Кібербулінг, мова ворожнечі, переслідування, поширення фейкових новин і маніпулятивного контенту	Розвиток критичного мислення, навички розпізнавання токсичних патернів поведінки; впровадження процедур конфіденційного повідомлення про інциденти та підтримки постраждалих
Фінансова безпека в цифровому середовищі	Онлайн-шахрайство, фішингові атаки, сумнівні інвестиційні пропозиції, боргові пастки	Здатність верифікувати фінансові сервіси, розпізнавати шахрайські схеми; розроблення освітніх модулів із цифрової фінансової грамотності у співпраці з банківським і фінтех-сектором
Цифровий добробут і психічне здоров’я	Залежність від соцмереж, інформаційне перевантаження, тривожність, викликана війною і токсичним контентом	Навички саморегуляції, управління часом онлайн, цифрового детоксу; посилення університетських служб психологічної підтримки з урахуванням цифрового контексту

Джерело: розроблено автором.

Запропонована структура дозволяє поєднати індивідуальні та інституційні рівні втручання: студенти отримують інструменти для самозахисту в цифровому середовищі, а університети – рамку для розробки політик, освітніх програм та сервісів підтримки. З позиції сталого розвитку важливо, що такі інтервенції базуються на партнерстві університетів із зовнішніми стейкхолдерами – ІТ-компаніями, фінансовими інституціями, правозахисними організаціями, регуляторами у сфері цифрових прав. Це дозволяє не лише оновлювати зміст навчальних програм, але й забезпечувати «вписаність» університетських практик у ширший цифровий та економічний контекст.

Україна як країна, що водночас перебуває в стані війни й прискореної цифрової трансформації, надає унікальне середовище для емпіричного дослідження цифрового виміру культури особистої безпеки. Молодь стикається з поєднанням воєнних, економічних та інформаційних загроз, що вимагає від університетів принципово нового рівня відповідальності й інституційної творчості. Впровадження цифрових модулів, політик та ресурсів дозволяє не лише підвищити безпеку й добробут студентів, а й сформувати

експортоспроможні моделі цифрової стійкості, релевантні для інших країн і регіонів, що переживають системні кризи.

Отже, цифровий вимір культури особистої безпеки є ключовою ланкою, що поєднує завдання сталого розвитку, цифрової економіки та модернізації вищої освіти. Університети, які інституційно вбудовують цифрову безпеку в свої стратегії, програми і практики, стають не лише постачальниками кваліфікованих кадрів для цифрової економіки, а й гарантами того, що ця економіка розвиватиметься на засадах відповідальності, поваги до прав людини та суспільної стійкості.

Список використаних джерел

1.Voronkova V., Nikitenko V., Oleksenko R., Andriukaitiene R., Kharchenko J., & Kliuienko E. Digital technology evolution of the industrial revolution from 4G to 5G in the context of the challenges of digital globalization. *TEM Journal.* 2023. Vol. 12(2). P. 732–742. https://doi.org/10.18421/tem122-17

2. Marienko V. The influence of information and communication technologies (ICT) on the development of society, humans, and technology: A social and philosophical analysis. *Educational Discourse: Collection of Scientific Papers*. 2024. Vol. 47(12). P. 61–72. https://doi.org/10.33930/ed.2019.5007.47(12)-6

3. Voronkova V., Nikitenko V., Oleksenko R., Cherep A., Cherep O., Harba H. The Creative Development of Green Ecotourism Concepta sa Sustainable Development Factor. *Revista dela universidad del Zulia.* 2024. Vol. 15(42). 370-388.

УДК 336.71

Е-ГРИВНЯ ЯК ІНСТРУМЕНТ ПІДВИЩЕННЯ ПРОЗОРОСТІ ФІНАНСОВИХ ОПЕРАЦІЙ У КОНТЕКСТІ ІНТЕГРАЦІЇ УКРАЇНИ ДО ЄВРОПЕЙСЬКОГО ФІНАНСОВОГО ПРОСТОРУ

Палига А. В.
здобувач вищої освіти ступеня бакалавр
Хмельницький університет управління та права імені Леоніла Юзькова, м. Хмельницький, Україна.

Пухальський В. В.
кандидат економічних наук, доцент,
Хмельницький університет управління та права імені Леоніда Юзькова, м. Хмельницький, Україна.

Етап інтеграції України у європейський економічний простір вимагає не лише гармонізації регуляторного поля, але й впровадження інноваційних технологічних рішень, здатних забезпечити високий рівень прозорості та контролю за фінансовими потоками. В умовах глобальної діджиталізації та зростання вимог до фінансового моніторингу, традиційні платіжні інструменти виявляють структурні обмеження щодо забезпечення повної відстежуваності транзакцій та ефективної протидії економічним злочинам. Виникає стратегічна необхідність впровадження цифрового інструменту, що поєднує надійність центрального банку з технологічними перевагами розподілених реєстрів. Таким інструментом є Е-гривня – цифрова валюта центрального банку (CBDC). Актуальність дослідження зумовлена необхідністю наукового обґрунтування потенціалу Е-гривні як ключового елемента модернізації платіжної інфраструктури, що критично важливе для прискорення євроінтеграційних процесів та підвищення довіри до українського фінансового ринку з боку міжнародних партнерів.