DOI: https://doi.org/10.32836/2521-666X/2021-72-11
УДК 35.746.1

Криклій О.А.
кандидат економічних наук, доцент,
Сумський державний університет
Боженко В.В.
кандидат економічних наук, доцент,
Сумський державний університет
Артюхов А.Є.
кандидат технічних наук, доцент,
Сумський державний університет

Kryklii Olena, Bozhenko Victoria, Artyukhov Artem
Sumy State University

ВПЛИВ ЦИФРОВОЇ ІНКЛЮЗІЇ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ КРАЇНИ [1]

IMPACT OF DIGITAL INCLUSION ON COUNTRY INFORMATION SECURITY

У статті узагальнено наявні підходи до розуміння концепту «інформаційна безпека країни». З'ясовано, що в його основі знаходиться концепт «інформаційна загроза». Уточнено зміст концепту «інформаційна загроза» та сформовано його багатовимірну класифікацію. Визначено, що специфічною загрозою інформаційній безпеці країни є інформаційна дискримінація. Доведено, що для нівелювання її негативного впливу необхідним є підвищення рівня цифрової інклюзії громадян та громади, що передбачає їх безпечну участь у всіх можливих аспектах функціонування інформаційного суспільства. Резюмовано, що досягнення цієї мети потребує формування довгострокової дорожньої карти розвитку інтелектуального капіталу країни, що вимагає значних інвестицій в освіту та формування оптимальної траєкторії освітніх трансформацій.

Ключові слова: *цифровізація, інформаційна безпека, інформаційна загроза, інформаційна дискримінація, цифрова інклюзія, освіта.*

В статье обобщены подходы к пониманию концепта «информационная безопасность страны». Установлено, что его основу формирует концепт «информационная угроза». Уточнено содержание концепта «информационная угроза» и сформирована его многомерная классификация. Определено, что специфической угрозой информационной безопасности страны является информационная дискриминация. Доказано, что для нивелирования ее негативного влияния необходимо повышение уровня цифровой инклюзии граждан и общества, что предполагает их безопасное участие во всех возможных аспектах функционирования информационного общества. Резюмировано, что достижение этой цели требует формирования долгосрочной дорожной карты развития интеллектуального капитала страны, значительных инвестиций в образование и формирование оптимальной траектории образовательных трансформаций.

Ключевые слова: *цифровизация, информационная безопасность, информационная угроза, информационная дискриминация, цифровая инклюзия, образование.*

In Ukraine, a fundamentally new landscape of threats to information security is now being formed, which is largely due to difficult geopolitical conditions, in particular, the exacerbation of information wars in the context of a military conflict with the Russian Federation, the growth of cyber threats and implemented cyberattacks, a low level of digital inclusion of the population, and the loss of innovative technological achievements. This requires not only a quick response to current threats, but also building the capacity to prevent them, in particular through the growth of digital inclusion. This will become the basis for countering information wars, stimulating economic growth, ensuring social stability, unity, cohesion and sustainability of communities and the country as a whole. The article examines approaches to understanding the concept of «information security of the country». Proceeding from the fact that it is based on the concept of «information threat», we investigate its essence and approaches to multidimensional classification. Information discrimination as a specific threat to the country's information security is being studied in depth. This is because it is a combination of the inaccessibility of ICTs and the lack of skills required to use them safely. To neutralize the negative impact of information discrimination, it is necessary to increase the level of digital inclusion of citizens and society, which implies their safe participation in all possible aspects of the functioning of the information society. To achieve this goal, it is necessary to form a long-term roadmap for the development of the country's intellectual capital, which requires significant investments in education and information skills based on the optimal trajectory of educational transformations that minimizes information threats. Educational institutions should be transformed into effective centres for the transfer of knowledge and technology for the growth of digital inclusion of citizens and communities in order to counter information threats and information wars, to ensure social stability, unity, cohesion and resilience of communities and the country as a whole.

Key words: *digitalization, information security, information threat, information discrimination, digital inclusion, education.*

[1] Виконано в рамках науково-дослідних тем: «Конвергенція економічних та освітніх трансформацій у цифровому суспільстві: моделювання впливу на регіональну та національну безпеку» та «Реформування системи освіти впродовж життя в Україні для запобігання трудовій еміграції: коопетиційна модель інституційного партнерства», що фінансуються за рахунок видатків загального фонду державного бюджету

Постановка проблеми. В Україні нині формується принципово новий ландшафт загроз інформаційній безпеці, що зумовлено складним геополітичним контекстом, загостренням інформаційних війн в умовах військового конфлікту з Російською федерацією, зростанням кіберзагроз та реалізованих кібератак, низьким рівнем цифрової інклюзії населення, втратою інноваційних технологічних надбань через кібервразливість тощо. Це потребує не лише швидкого реагування на поточні загрози, а й формування потенціалу для їх превенції, зокрема шляхом зростання цифрової інклюзії населення для протидії інформаційним війнам, забезпечення соціальної стабільності, єдності, згуртованості та стійкості громад та країни у цілому. Особливу увагу у цьому контексті необхідно приділити формуванню концептуальної моделі та економіко-математичному обґрунтуванню зв'язку цифрової інклюзії населення з рівнем інформаційної безпеки країни та регіону.

Ураховуючи зазначене вище, а також фрагментарність наявного наукового доробку у цій сфері, значну специфічність ендогенної природи конвергентних процесів у ланцюзі «освіта – цифрова інклюзія населення – інформаційна безпека країни та регіону», їх суттєву чутливість до екзогенних кібер- та безпекових викликів, розв'язання цієї проблеми є актуальним та має практичну спрямованість.

Аналіз останніх досліджень і публікацій. Аналіз наукових досліджень у цій сфері дав змогу виявити декілька кластерів, що об'єднують праці аналогічного спрямування. Найбільший науковий доробок, представлений працями К. Чаби, З.В. Белласа [1], С. Лєонова, Г. Яровенко, О. Кузьменко, М. Стумпо та ін. [2; 5; 7; 10], О. Солодкої [8], Т. Ткачука [9], сконцентровано у першому кластері, присвяченому дослідженням інформаційної безпеки як складової частини національної безпеки, її оцінюванню та механізмам забезпеченням.

Трендовий аналіз із використанням інструментарію Google Trends (рис. 1) дав змогу виявити постійний інтерес до цієї тематики з максимальною концентрацією уваги до неї в таких країнах, як США, Великобританія та Індія.

Національну інформаційну безпеку досліджують у контексті національної безпеки, кібервійн, інформаційних злочинів, розвитку технологій та інфраструктури, кіберризиків, цифрової інклюзії. Напрацювання цього напряму потребують продовження у сфері моделювання взаємозв'язків між рівнем інформаційної безпеки, цифровою інклюзією населення та розвитком системи освіти з урахуванням часових лагів, конвергенції, явних та латентних економічних та соціальних ефектів.

Другий кластер [11–17] фокусується на дослідженні цифрової (електронної) інклюзії (E-Inclusion) у контексті розвитку інформаційного суспільства (А. Абдул [11]), забезпечення соціальної стабільності, високого рівня якості життя (М.А. Алі, К. Алам, Б. Тейлор, С. Рафік [12]), інклюзивного зростання в країні (А. Аслам, А. Навід, Г. Шаббір [13]), розуміння вимірювань та причин цифрових розривів та інструментарію їх мінімізації (І. Мірошниченко, Є. Морозова та Є. Мещерякова [15]; А. Ндуму, Л.М. Мон, З. Фан [17]), специфіки взаємозв'язків між індивідуальними, цифровими та економічними аспектами ринкових відносин (В.А. Бейї [13]). М.Р. Селеш та М. Сіміонеску [16] досліджували цифрові розриви в контексті регіональних закономірностей та рушіїв цифрової економіки ЄС.

Як свідчать результати трендового аналізу з використанням інструментарію Google Trends, у світі наявний постійний інтерес до цієї тематики. Країнами-лідерами з найбільшою кількістю запитів є Великобританія, Аргентина, Мексика, Австралія та Індія. Достатньо активно цифрова інклюзія досліджується в контексті формування стратегій забезпечення цифрової інклюзії у цілому та фінансової інклюзії зокрема, вимірювання цифрової інклюзії (індекс цифрової інклюзії), ролі освіти в підвищенні рівня цифрової інклюзії тощо.

Попри вагомість отриманих результатів у наукових працях цього кластера практично не обґрунтовано зворотні впливи та зв'язок низького рівня цифрової ін-

Рис. 1. Динаміка пошукових запитів у Google щодо проблем забезпечення інформаційної безпеки країни з урахуванням рівня цифрової інклюзії за період 2004 р. – лютий 2021 р.

Джерело: побудовано авторами з використанням Google Trends

клюзії населення із загостренням безпекових викликів, насамперед у контексті забезпечення інформаційної безпеки на національному та регіональному рівнях.

Третій кластер публікацій присвячений дослідженню рівня цифровізації суспільства та оцінюванню його впливу на соціальні, економічні, безпекові характеристики країни. Так, у звіті «DIGITAL 2020: глобальний цифровий огляд» наводяться аналітичні дані щодо цифровізації життєдіяльності та рівня цифрової інклюзії й цифрової дискримінації в країнах світу з виявленням значних гендерних та географічних дисбалансів [18].

У звіті Конференції ООН із торгівлі та розвитку (UNCTAD) [19] визначено шляхи розвитку цифрових навичок та їх використання для підтримки сталого розвитку, трансформації економіки, виробничих секторів та ринків, у тому числі через технологічну конвергенцію та рекомбінацію, підвищення громадянської та соціальної активності населення.

У звіті ОЕСР [20] систематизовано тенденції, можливості та проблеми цифровізації суспільства, але триалектичний системний взаємозв'язок освіти, економіки та цифровізації залишився не окресленим, у тому числі через призму регіональної та національної безпеки.

Для науковців, які досліджують тематику інформаційної безпеки, зокрема в контексті впливу на неї, значний інтерес становлять спеціальні індекси, що дають змогу оцінити рівень цифровізації, розвитку цифрової економіки та окремих її елементів, а також побудувати рейтинги країн, зокрема глобальний індекс кібербезпеки, індекс розвитку інформаційно-комунікаційних технологій, індекс мережевої готовності, світовий індекс цифрової конкурентоспроможності, індекс цифрового розвитку та ін.

Мета статті полягає в обґрунтуванні концептуального зв'язку цифрової інклюзії населення із забезпеченням інформаційної безпеки країни.

Виклад основного матеріалу. Для досягнення мети дослідження вважаємо за доцільне уточнити сутність концептів «інформаційна безпека» та «цифрова інклюзія», а також систематизувати чинники, що впливають на їх рівень у країні в поточний момент часу та на перспективу. Результатом цього стане обґрунтування концептуального зв'язку цифрової інклюзії населення з рівнем інформаційної безпеки (ІБ) країни.

Узагальнивши науковий доробок із цієї тематики, ми визначили, що єдиного підходу до тлумачення концепту ІБ не сформовано і вона розглядається за декількома підходами (рис. 2).

Як свідчать наведені підходи, в основі всіх підходів до тлумачення концепту «інформаційна безпека» – інформаційні (кіберзагрози) загрози, що створюють небезпеку порушення ІБ.

Адаптуючи загальне розуміння поняття «загроза» до завдань дослідження, визначимо, що загроза ІБ країні – це потенційно можлива випадкова або навмисна подія, дія (вплив), процес або явище, що можуть призвести до втрати критично важливих приватних, дер-

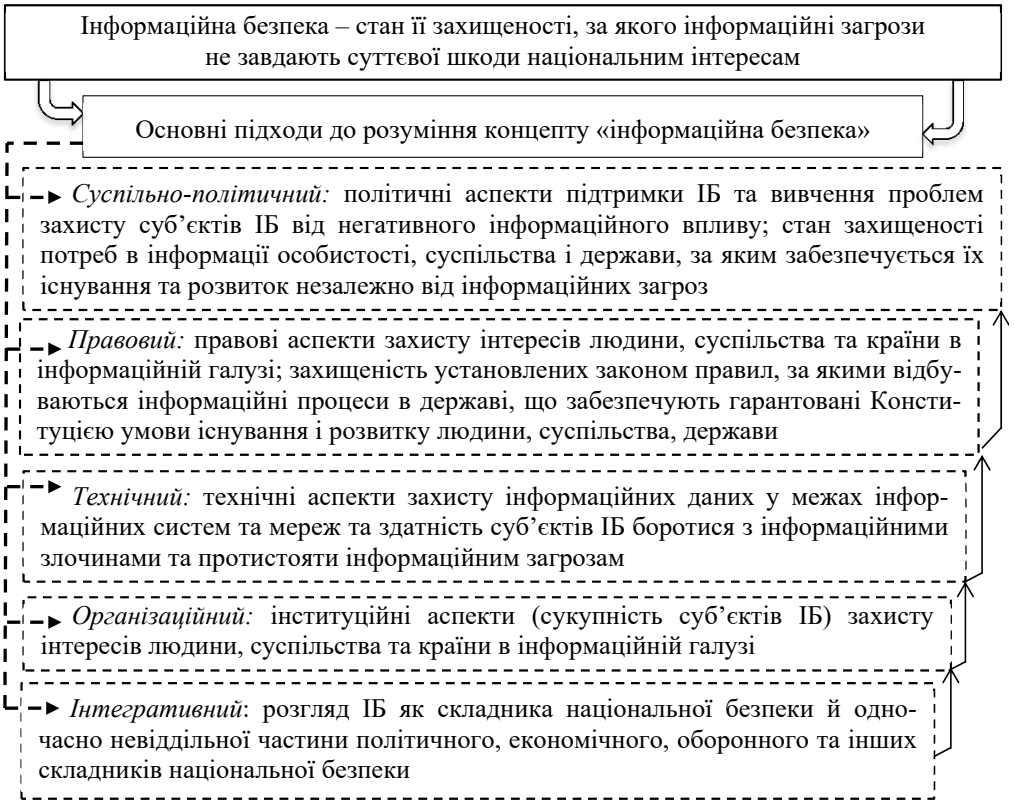

Рис. 2. Підходи до визначення концепту «інформаційна безпека»

Джерело: узагальнено авторами

жавних або загальнодоступних інформаційних активів та інформаційної інфраструктури чи порушення властивостей інформаційних активів (конфіденційності, цілісності, доступності). Їх базову класифікацію наведено в табл. 1.

Поглиблене вивчення джерел загроз ІБ країни дав змогу виявити, що причиною генерації значної кількості з них є людський фактор, що є, мабуть, найбільшим викликом під час розроблення ефективної стратегії запобігання ним.

Це джерело загроз ІБ країни є комплексним та включає:

1) ненавмисні дії:

– помилкові, випадкові, необдумані, без злого наміру та корисливих цілей порушення встановлених регламентів збору, обробки та передачі інформації;

– помилки, допущені під час проєктування інформаційних систем та систем захисту, помилки в програмному забезпеченні, відмови та збої технічних засобів (у тому числі засобів захисту інформації та контролю ефективності захисту);

– інші дії під час експлуатації інформаційних систем, що призводять до непродуктивних витрат часу та ресурсів, розголошення конфіденційних даних, втрати інформації або порушення працездатності окремих робочих станцій, підсистем або в цілому всієї системи;

2) навмисні (у корисливих цілях, з примусу третіми особами, зі злим умислом тощо) дії інсайдерів організації, злочинних груп та формувань, політичних та економічних структур, окремих осіб. Вони, зокрема, включають:

– кібератаки на критичну інфраструктуру країни, у тому числі кіберфізичні атаки на електричні мережі, транспортні системи, водоочисні споруди тощо, що можуть здійснюватися як окремими злочинними групами, так і фінансуватися на державному рівні;

– кібершпигунство;

– соціальну інженерію як сукупність інструментарію психологічних маніпуляцій у здійсненні несанкціонованих дій або розголошення конфіденційної інформації (фішинг, спір-фішинг, фармінг, претекстинг, скрімінг та ін.);

– діяльність злочинних груп та формувань, політичних та економічних структур, а також окремих осіб із добування інформації, нав'язування неправдивої інформації, порушення працездатності інформаційних систем у цілому та її окремих компонентів, підбурю-

Таблиця 1

Багатовимірна класифікація інформаційних загроз

Ознака	Вид загрози
Методи проникнення	
Локалізація причин	- зовнішні; - внутрішні.
Сфера виникнення	- економічна; - політична; - оборонна; - міжнародна; - соціальна; - науково-технічна;- екологічна; - культурна
Походження	- природні, що характеризуються впливом на об'єкт захисту фізичних процесів або стихійних природних явищ, що не залежать від людини; - техногенні (аварії на інженерних мережах і спорудах життєзабезпечення, аварії головних серверів системи управління національною безпекою тощо); - людські, що характеризуються впливом на об'єкт захисту діяльністю людини, у тому числі результати соціальної інженерії (фішинг, фармінг, претекстинг, скрімінг та ін.) та інформаційна дискримінація
Мотивація	- ненавмисна (помилкові, випадкові, необдумані, без злого наміру та корисливих цілей) дії інсайдерів та третіх сторін; - навмисна (у корисливих цілях, із примусу третіми особами, зі злим умислом тощо) дії інсайдерів, злочинних груп та формувань, політичних і економічних структур, окремих осіб
Спосіб реалізації	- розголошення; - витік; - несанкціонований доступ
Сформованість	- реальні; - потенційні
Прогнозованість	- прогнозовані; - не прогнозовані
Ймовірність виникнення	- реальна; - ймовірна; - малоймовірна; неймовірна
Можливість нейтралізації	- можливо нейтралізувати; - можливо частково нейтралізувати; - нейтралізувати неможливо
Вплив загроз	
Ступінь впливу	- пасивні без впливу на стан інформаційної системи; - активні з порушенням нормального процесу функціонування інформаційної системи
Характер впливу	- явна, пряма (загрози, реалізація яких порушує безпеку інформаційних активів); - неявна, опосередкована (загрози, що створюють умови для появи прямих загроз)
Масштаб наслідків	- катастрофічні; - критичні; - середні; - незначні
Локалізація наслідків	- світові; - загальнонаціональні; - регіональні; - локальні
Вид порушення ІБ в результаті реалізації загрози	втрата, знищення, викрадення, викривлення або розголошення інформації, витік інформації, модифікація змісту, порушення конфіденційності, порушення логічної цілісності, порушення прав власності на інформацію, порушення фізичної цілісності, порушення режиму роботи інформаційних систем тощо

Джерело: узагальнено авторами

вання до расової, етнічної або релігійної ненависті, пропаганди тоталітарних сект та ін.;

– спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм.

Ми погоджуємося з твердженням Ю. Ткачука [9], який виділив таку специфічну загрозу ІБ країни та суспільства у цілому, як «…інформаційна дискримінація, яка виявляється в поділі людей на тих, які мають доступ до інформації, і тих, які його не мають, адже від цього залежить можливість формування неспотвореної «картини світу». Цілком очевидним є той факт, що подолання інформаційної дискримінації сприятиме підвищенню рівня освіченості населення, особливо з віддалених регіонів та соціально вразливих верств, у тому числі рівня їх цифрової грамотності. Це, своєю чергою, підвищить рівень інформаційної безпеки країни, слугуватиме соціальній мобільності, економічному зростанню, поглибленню демократії.

Сьогодні у зв'язку зі швидким поширенням мобільного Інтернету акцент в інформаційній дискримінації із суто проблеми доступу до ІКТ переноситься до сфери здатності громадян безпечно користуватися інформаційно-комунікаційними інструментами (перехід від дискримінації в доступі та підключенні до ІКТ до розриву в знаннях [21]).

У міру появи нових векторів інформаційних загроз зростатимуть розриви та інформаційна дискримінація між тими суб'єктами, які мають знання та ресурси, щоб захиститися від кіберзагроз, і тими, хто їх не має. Множинний регресійний аналіз у різних країнах засвідчив, що рівні доходів та освіти визначені як найпотужніші пояснювальні змінні для доступу до ІКТ та його використання [22]. У подальшому навички розуміння інформаційних загроз та фінансові ресурси для захисту від цих загроз матимуть вирішальне значення для інформаційної безпеки як на індивідуальному, так і національному, глобальному рівнях.

Проблема інформаційної дискримінації та, як наслідок, інформаційної безпеки поглиблюється в країнах із низьким рівнем доходів, до яких належить і Україна. Це зумовлено тим, що фактори доступності до ІКТ та недостатність навичок, необхідних для їх використання, інтенсифікуються через взаємовплив та співзалежність. Цей розрив у знаннях та ресурсах лише збільшить наявні економічні та соціальні розбіжності й інформаційні загрози.

На подолання інформаційної дискримінації спрямована цифрова інклюзія, що розглядається як використання інформаційно-комунікаційних технологій (ІКТ) для досягнення широких цілей соціальної інклюзії та передбачає участь громадян та громад у всіх можливих аспектах функціонування інформаційного суспільства.

Для цього потрібно забезпечити повний доступ до ІКТ, доступність та зручність використання засобів та послуг ІКТ, а також сформувати здатність та навички для всіх без винятку категорій осіб незалежно від їхніх особливостей (національності, раси, статків, статі, соціального становища, функціональних обмежень, регіону проживання тощо) користуватися інструментами ІКТ.

Зважаючи на зазначене вище, для підвищення рівня цифрової інклюзії обов'язковою вимогою є довгострокова державна підтримка розвитку інтелектуального капіталу країни, що вимагає значних інвестицій в освіту та формування інформаційних навичок. Це передбачає формування комплексу заходів щодо підвищення рівня цифрової грамотності громадян через сталі партнерства з освітніми установами, створення безплатного навчального онлайн-порталу, а також запровадження стимулів для заохочення приватних ініціатив до створення центрів, проведення курсів, надання навчальних ресурсів тощо.

Заклади освіти мають трансформуватися в ефективні центри трансферу знань та технологій для зростання цифрової інклюзії громадян та громад із метою протидії інформаційним загрозам та інформаційним війнам, забезпечення соціальної стабільності, єдності, згуртованості та резільєнтності громад та країни у цілому.

Висновки. Інформаційна безпека країни – це такий стан її захищеності, за якого інформаційні загрози не завдають суттєвої шкоди національним інтересам.

За результатами проведеного дослідження визначено, що інформаційна безпека України знаходиться під впливом значної кількості зовнішніх та внутрішніх інформаційних загроз, що можуть призвести до втрати критично важливих приватних, державних або загальнодоступних інформаційних активів та інформаційної інфраструктури чи до порушення властивостей інформаційних активів (конфіденційності, цілісності, доступності) та, як наслідок, до зниження рівня національної безпеки країни.

З'ясовано, що специфічною загрозою інформаційній безпеці країни є інформаційна дискримінація як поєднання недоступності до ІКТ та недостатності навичок, необхідних для їх безпечного використання. Для нівелювання її негативного впливу необхідним є підвищення рівня цифрової інклюзії громадян та громади, що передбачає їх участь у всіх можливих аспектах функціонування інформаційного суспільства.

Досягнення цієї мети потребує формування довгострокової дорожньої карти розвитку інтелектуального капіталу країни, що вимагає значних інвестицій в освіту та формування інформаційних навичок на основі оптимальної траєкторії освітніх трансформацій, за якої мінімізуються загрози інформаційній безпеці країни, зростають резільєнтність місцевих громад та регіональна безпека, нівелюються загрози та вдало використовуються нові можливості, зумовлені цифровізацією економіки та суспільства.

Список літератури:

1. Csaba K., Bellász Z.V. Terrorism and the information security of media content with special regard to ISIS, the Balkans and Russia. *SocioEconomic Challenges.* 2017. № 1(1). P. 13–19.

2. The Innovative Approach to Increasing Cybersecurity of Transactions Through Counteraction to Money Laundering / S. Lyeonov et al. *Marketing and Management of Innovations.* 2019. № 3. P. 308–326. URL: https://doi.org/10.21272/mmi.2019.3-24 (дата звернення: 27.02.2021).

3. Milon K., Nur-Al-Ahad Md., Monjurul Alam A.B.M. The Deployment of Next Generation Access Network in the EU: Facts and Analysis of Regulatory Issues. *Business Ethics and Leadership.* 2018. № 2(4) P. 6–17. DOI: https:// doi.org/10.21272/bel.2(4).6-17.2018 (дата звернення: 27.02.2021).

4. Artificial Intelligence: Serving American Security and Chinese Ambitions / H. Obeid et al. Financial Markets, *Institutions and Risks.* 2020. № 4(3). P. 42–52. DOI: https://doi.org/10.21272/fmir.4(3).42-52.2020 (дата звернення: 27.02.2021).

5. Yarovenko H., Kuzmenko O., Stumpo M. DEA-Analysis Of The Effectiveness Of The Country's Information Security System. *SocioEconomic Challenges.* 2020. № 4(3). P. 142–153. DOI: https://doi.org/10.21272/sec.4(3) (дата звернення: 27.02.2021).

6. Yarovenko H., Kuzmenko O., Stumpo M. Strategy for Determining Country Ranking by Level of Cybersecurity. *Financial Markets, Institutions and Risks.* 2020. № 4(3). P. 124–137. DOI: https://doi.org/10.21272/fmir.4(3).124-137.2020 (дата звернення: 27.02.2021).

7. Yarovenko H. Evaluating the threat to national information security. *Problems and Perspectives in Management*. 2020. № 18(3). P. 195–210. DOI: https:// doi.org/10.21511/ppm.18(3).2020.17 (дата звернення: 27.02.2021).

8. Солодка О. Інформаційний суверенітет та інформаційна безпека України: діалектика понять. *Evropský politický a právní diskurz.* 2020. Sv. 7. Vyd. 6. C. 233–239. DOI: https://doi.org/10.46340/eppd.2020.7.6.29 (дата звернення: 27.02.2021).

9. Ткачук Т.Ю. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз. *Підприємництво, господарство і право.* 2017. № 10. С. 182–186.

10. Яровенко Г.М. Бібліометричний аналіз досліджень інформаційної безпеки в розрізі розвитку національної економіки. *Інтернаука. Серія: «Економічні науки».* 2020. № 8(40). С. 53–63. URL: https://doi.org/10.25313/2520-2294-2020-8-6245 (дата звернення: 27.02.2021).

11. Abdul A. Digital inclusion challenges in Bangladesh: the case of the National ICT Policy. *Contemporary South Asia.* 2020. № 28:3. P. 304–319. DOI: https://doi.org/10.1080/09584935.2020.1793912 (дата звернення: 27.02.2021).

12. Does digital inclusion affect quality of life? Evidence from Australian household panel data / M.A. Ali et al. *Telematics and Informatics.* 2020. Volume 51. DOI: https://doi.org/10.1016/j.tele.2020.101405.

13. Aslam A., Naveed A., Shabbir G. Is it an institution, digital or social inclusion that matters for inclusive growth? A panel data analysis. *Qual Quant.* 2021. № 55. P. 333–355. DOI: https://doi.org/10.1007/s11135-020-01008-3 (дата звернення: 27.02.2021).

14. Beyi W.A. The Trilogy of a Digital Communication between the Real Man, His Digital Individual and the Market of the Digital Economy. *SocioEconomic Challenges.* 2018. № 2(2). P. 66–74. DOI: https://doi.org/10.21272/sec.2(2).66-74.2018 (дата звернення: 27.02.2021).

15. Miroshnichenko I., Morozova E., Meshcheryakova E. Policy for Overcoming Digital Inequality: Structure, Actors and Technologies. *6th International Conference on Economics, Management, Law and Education (EMLE 2020).* DOI: https://doi.org/10.2991/aebmr.k.210210.065 (дата звернення: 27.02.2021).

16. Szeles M.R., Simionescu M. Regional patterns and drivers of the EU digital economy. *Social Indicators Research*. 2020. № 150(1). № 95–119. DOI: https://doi.org/:10.1007/s11205-020-02287-x (дата звернення: 27.02.2021).

17. E-inclusion or digital divide: an integrated model of digital inequality / B.Yu et al. *Journal of Documentation.* 2018. № 74. DOI: https://doi.org/10.1108 /JD-10-2017-0148 (дата звернення: 27.02.2021).

18. Digital 2020 Global Digital Overview. URL: https://wearesocial.com/digital-2020 (дата звернення: 02.03.2021).

19. Building Digital Competencies to Benefit from Frontier Technologies. UNCTAD New York, United Nations Publications, 2019. URL: https://unctad.org/en/pages/PublicationWebflpublicationid=2449 (дата звернення: 27.02.2021).

20. Going Digital: Shaping Policies, Improving Lives, OECD Publishing, Paris, 2019. URL: https://www.oecd-ilibrary.org/sites/9789264312012-en/index.html?itemId=/content/publication/9789264312012-en (дата звернення: 27.02.2021).

21. Graham M. Time machines and virtual portals: The spatialities of the digital divide. *Progress in Development Studies.* 2011. № 11(3). P. 211–227. CiteSeer X 10.1.1.659.9379. DOI:10.1177/146499341001100303.S2CID 17281619.

22. Hilbert M. When is Cheap, Cheap Enough to Bridge the Digital Divide? Modeling Income Related Structural Challenges of Technology Diffusion in Latin America. *World Development.* 2010. № 38(5). P. 756–770. DOI: doi:10.1016/j.worlddev.2009.11.019 (дата звернення: 27.02.2021).

References:

1. Csaba K., Bellász Z.V. (2017) Terrorism and the information security of media content with special regard to ISIS, the Balkans and Russia. *SocioEconomic Challenges,* no. 1(1), pp. 13–19. DOI: http://doi.org/10.21272/sec.2017.1-02.

2. Lyeonov S., Kuzmenko O., Yarovenko H., Dotsenko T. (2019) The Innovative Approach to Increasing Cybersecurity of Transactions Through Counteraction to Money Laundering. *Marketing and Management of Innovations*, no. 3, pp. 308–326. DOI: http://doi.org/10.21272/mmi.2019.3-24.

3. Milon K., Nur-Al-Ahad Md., Monjurul Alam A.B.M. (2018) The Deployment of Next Generation Access Network in the EU: Facts and Analysis of Regulatory Issues. *Business Ethics and Leadership,* no. 2(4), pp. 6–17. DOI: http://doi.org/10.21272/bel.2(4).6-17.2018.

4. Obeid H., Hillani F., Fakih R., Mozannar K. (2020) Artificial Intelligence: Serving American Security and Chinese Ambitions. *Financial Markets, Institutions and Risks*, no. 4(3), pp. 42–52. DOI: https://doi.org/10.21272/fmir.4(3).42-52.2020.

5. Yarovenko H., Kuzmenko O., Stumpo M. (2020) DEA-Analysis Of The Effectiveness Of The Country's Information Security System. *SocioEconomic Challenges,* no. 4(3), pp. 142–153. DOI: https://doi.org/10.21272/sec.4(3).142-153.2020.

6. Yarovenko H., Kuzmenko O., Stumpo M. (2020) Strategy for Determining Country Ranking by Level of Cybersecurity. *Financial Markets, Institutions and Risks*, no. 4(3), pp. 124–137. DOI: https://doi.org/10.21272/fmir.4(3).124-137.2020.

7. Yarovenko H. (2020) Evaluating the threat to national information security. *Problems and Perspectives in Management*, no. 18(3), pp. 195–210. DOI: https://doi.org/10.21511/ppm.18(3).2020.17.

8. Solodka O.M. (2020) Zabezpechennya informatsiynogo suverenitetu derzhavi: pravoviy diskurs [Ensuring the information sovereignty of the state: legal discourse]. *InformatsIya i pravo,* no. 1(32), pp. 80–87.

9. Tkachuk T. (2017) Suchasni zahrozy informatsiyniy bezpetsi derzhavy: teoretyko-pravovyy analiz [Modern threats to information security of the state: theoretical and legal analysis]. *Pidpryyemnytstvo, hospodarstvo i pravo,* no. 10, pp. 182–186.

10. Yarovenko H.M. (2020) Bibliometrychnyy analiz doslidzhen informatsiynoyi bezpeky v rozrizi rozvytku natsionalnoyi ekonomiky [Bibliometric analysis of information security research in terms of national economy development]. *Mizhnarodnyy naukovyy zhurnal «Internauka». Seriya: «Ekonomichni nauky»*, no. 8(40), pp. 53–63. DOI: https://doi.org/10.25313/2520-2294-2020-8-6245.

11. Abdul A. (2020) Digital inclusion challenges in Bangladesh: the case of the National ICT Policy. *Contemporary South Asia*, no. 28:3, pp. 304–319. DOI: https://doi.org/10.1080/09584935.2020.1793912.

12. Ali M.A, Alam K., Taylor B., Rafiq S. (2020) Does digital inclusion affect quality of life? Evidence from Australian household panel data. *Telematics and Informatics,* no. 51. DOI: https://doi.org/10.1016/j.tele.2020.101405.

13. Aslam A., Naveed A., Shabbir G. (2021) Is it an institution, digital or social inclusion that matters for inclusive growth? A panel data analysis. *Qual Quant,* no. 55, pp. 333–355. DOI: https://doi.org/10.1007/s11135-020-01008-3.

14. Beyi W.A. (2018) The Trilogy of a Digital Communication between the Real Man, His Digital Individual and the Market of the Digital Economy. *SocioEconomic Challenges,* no. 2(2), pp. 66–74. DOI: https://doi.org/10.21272/sec.2(2).66-74.2018.

15. Miroshnichenko I., Morozova E., Meshcheryakova E. (2021, February) Policy for Overcoming Digital Inequality: Structure, Actors and Technologies. *In 6th International Conference on Economics, Management, Law and Education (EMLE 2020)* (pp. 401–405). Atlantis Press.

16. Szeles M.R., Simionescu M. (2020) Regional Patterns and Drivers of the EU Digital Economy. *Social Indicators Research,* pp. 1–25.

17. Yu B., Ndumu A., Mon L.M., Fan Z. (2018) E-inclusion or digital divide: an integrated model of digital inequality. Journal of Documentation.

18. Digital 2020 Global Digital Overview (2020). Available at: https://wearesocial.com/digital-2020.

19. Building Digital Competencies to Benefit from Frontier Technologies (2019). UNCTAD New York, United Nations Publications. Available at: https://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=2449.

20. Lesher M., Gierten D., Attrey A., Carblanc A., Ferguson S. (2019) Going digital: Shaping policies, ımproving lives.

21. Graham M. (2011) Time machines and virtual portals: The spatialities of the digital divide. *Progress in development studies*, no. 11(3), pp. 211–227.

22. Hilbert M. (2010) When is cheap, cheap enough to bridge the digital divide? Modeling income related structural challenges of technology diffusion in Latin America. *World Development,* no. 38(5), pp. 756–770.