DOI: https://doi.org/10.18371/fp.1(33).2019.177107

УДК 338.2:004.9

КІБЕРЗАГРОЗИ В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ

ПАНТЄЛЄЄВА Наталія Миколаївна,
доктор економічних наук, доцент
заступник директора Черкаського інституту
ДВНЗ «Університет банківської справи»
ORCID ID: 0000-0001-6457-6912
e-mail: nnpanteleeva2017@gmail.com

РОМАНОВСЬКА Людмила
науковий співробітник
ДВНЗ «Університет банківської справи»
e-mail: ludmila08romanovska@gmail.com

РОМАНОВСЬКА Марія
курсант Військового інституту
телекомунікацій та інформатизації
імені Героїв Крут

Анотація. *Узагальнено теоретичні положення дискусійного тлумачення поняття «кібербезпека» за системним і суб'єктно-об'єктним підходами; вивчено позицію міжнародного професійного товариства та урядів країн світу щодо стратегічного управління кібербезпекою; узагальнено характеристичні ознаки типологізації кіберзагроз, визначено об'єкти, сфери та тенденцій їх поширення і руйнівного впливу; виявлено поліаспектну природу цифрових технологій стосовно вразливості, стійкості та здатності до протидії кіберзагрозам; розкрито інституційну інфраструктуру та проведено критичний аналіз концептуальних документів національної системи кібербезпеки.*

Ключові слова: *цифрова економіка, цифрові технології, кібербезпека, кіберзагрози, криптовалюта, блокчейн, штучний інтелект.*

Аннотация. *Обобщены теоретические положения дискуссионного толкования понятия «кибербезопасность» за систем-ным и субъектно-объектным подходами; изучено позицию международного профес-сионального сообщества и правительств стран мира по стратегическому управлению кибербезопасностью; обобщенно характерные признаки типологизации киберугроз, определены объекты, сферы и тенденций их распространения и разрушительного воздействия; выявлено полиаспектну природу цифровых технологий применительно уязви-мости, устойчивости и способности к противодействию киберугрозами; раскры-то институциональную инфраструктуру и проведен критический анализ концептуа-льных документов национа-льной системы кибербезопасности.*

Ключевые слова: *цифровая экономика, цифровые технологии, кибербезопасность, киберугрозы, криптовалюта, блокчейн, искусственный интеллект.*

Постановка проблеми. Сучасним драйвером соціально-економічного розвитку, набуття конкурентоспроможності та підвищення якості життя як для окремої країни, так і всього світу виступає цифрова економіка. Процеси цифровізації стрімко поширюються та набувають особливої значущості в усіх сферах життєдіяльності, водночас породжуючи нові загрози і виклики, відкриваючи невідомі раніше можливості для зловживань і правових порушень. Тому у світовому порядку денному постало складне питання забезпечення кібербезпеки, розробки та здійснення ефективних заходів щодо боротьби з кіберзлочинністю. Його вирішення потребує системного і комплексного підходів, адже цифрова економіка будується на широкому переліку ключових цифрових технологій та інфраструктурі, прикладна реалізація яких у тій або інший сферах формує і розширює контури цифрового середовища, але поряд з наданням нової функціональності посилює ризики.

Аналіз останніх досліджень і публікацій. Проблемним аспектам інформаційної та кібербезпеки присвятили свої наукові праці зарубіжні та вітчизняні вчені, зокрема: О.А. Баранов, С. Бейделман, П. Вуллей, М.В. Грайворонський, М.В. Гуцалюк, О.Д. Довгань, І.М. Доронін, Д. Дубов, О.О. Золотар, Дж. Ліпман, А.І. Марущак, Г.В. Новицький, І. Рус, А.В. Тарасюк, Н.А. Ткачук, В.М. Фурашев, А. Хілдрет та ін.

Мета статті полягає в узагальненні теоретичних положень понятійного апарату та визначення стратегічних позицій країн світу у сфері кібербезпеки, узагальнення характеристичних ознак типологізації кіберзагроз, виявлення поліаспектної природи цифрових технологій стосовно вразливості та здатності до протидії кіберзагрозам.

Виклад основних результатів. Враховуючи, що забезпечення кібербезпеки входить до питань національної безпеки, але цим не обмежується, країнами світу прийнято відповідні стратегії на засадах широкого міжнародного співробітництва, оцінку змісту деяких з них стосовно ефективності заходів реалізації достатньо повно розкрив М.В. Гуцалюк [1]. Такі концептуальні документи перш за все спираються та так або інакше розкривають сутність поняття «кібербезпека» (cybersecurity), формуючи теоретичний базис побудови національних систем безпеки (табл. 1).

Варто відмітити, що в науковій спільноті та професійному середовищі на сьогодні відсутня єдність позицій щодо сутності поняття «кібербезпека».

Так, І. Рус вважає, що за системним підходом кібербезпека охоплює захист електронного обладнання, програмне забезпечення обробки даних та інформації, а як концепція включає інформаційну безпеку, поширюється на мобільні пристрої та інтелектуальне обладнання, структуровану та неструктуровану інформацію, якою воно управляє [7, с.11-12].

На думку В.М. Фурашева, «кібербезпека – стан спроможності людини, суспільства і держави

запобігання та уникнення спрямованого, в першу чергу – несвідомого, негативного впливу (управління) інформації» [8, с.163], але в подальшому, спираючись на поняття «простір» та «кібернетика», автор уточнює поняття «кіберпростір» [8, с.164]. Крім того, порівнюючи за суб'єктно-об'єктним підходом поняття «кіберпростір» та «інформаційний простір», «кібербезпека» та «інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, якому запобігається завдання шкоди…», В.М. Фурашев дійшов висновку, що останні поняття сутнісно тотожні.

Таблиця 1

Розуміння поняття «кібербезпека» в деяких стратегіях країн світу

Країна	Кібербезпека – це
Україна [2]	захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі
США [3]	можливість захищати і боронити використання кіберпростору від кібератак
Велика Британія [4]	захист інтересів в кіберпросторі та реалізація ширшої політики безпеки за допомогою використання багатьох можливостей, які пропонує кіберпростір, не перешкоджаючи використання нових технологій для інновацій та розвитку країни
Іспанія [5, с.4]	нормативна база та інфраструктура, яка об'єднує і координує всі установи, побудована за принципом ефективності та стійкості у використанні ресурсів, гарантуючи оптимальні можливості захисту, виявлення, аналізу, розслідування, відновлення і реагування інформаційних і телекомунікаційних систем на можливі кібератаки.
Нідерланди [6, с.6]	захист «усього», що є вразливим, оскільки воно пов'язане з інформаційними та комунікаційними технологіями або залежить від них іншим чином.

Джерело: сформовано авторами за результатами опрацювання визначених джерел

О.А. Баранов надає вузьке і широке визначення поняття «кібербезпека»: 1) «інформаційна безпека в умовах використання комп'ютерних систем та/або телекомунікаційних мереж»; 2) «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» [9, с.61]. Тобто, автор в першому підході ототожнює кібербезпеку з інформаційною безпекою, а за другим – стверджується, що

це «стан захищеності», тобто стала характеристична властивість.

Стандарт ISO/IEC 27032 «Guidelines for cybersecurity» також визначає кібербезпеку як властивість захищеності активів від загроз конфіденційності, цілісності, доступності у кіберпросторі [10].

Проте, на нашу думку, стан захищеності є важливим підсумком конкретних процесів і дій, які створюють умови досягнення рівня безпеки та забезпечення його сталості в часі.

Підтримуємо позицію, що надана в РекомендаціяхX.1205 «Overview of Cybersecurity» кібербезпека – «набір засобів, стратегії, принципи забезпечення безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, професійна підготовка, практичний досвід, страхування і технології, які можуть бути використані для захисту кіберсередовища, ресурсів організації і користувача» [11, с.2].

Такий контекст, але дещо вузько, підтримує також Конфедерація цифрового бізнесу (Білорусь) розглядає кібербезпеку як створення і реалізацію заходів щодо захисту систем, мереж і різних додатків від комп'ютерних (цифрових) атак [12].

Отже, на нашу думку, поняття «кібербезпека» є комплексним, що поєднує у своїй сутності предметну основу кіберпростору та процесну функціональність механізму захисту, спирається на системний та інституційний підходи, принципи ефективності, надійності, оптимальності.

Побудова ефективної системи кібербезпеки передбачає розуміння видів кіберзагроз та їх руйнівних властивостей, які мають глобальний характер і стають все більш небезпечними, а поряд із технічним функціоналом завжди мають мотивуючий фактор (табл. 2). Типологізація кіберзагроз є відкритою, що цілком закономірно пов'язано з прогресивним розвитком технологій. З цих позицій у класифікації моделей кібератак можна виокремити такі, що використовують вразливості та діють на: мережеву інфраструктуру; протоколи транспортного і мережевого рівнів, передачі даних; конфігурацію сервера; стандартне програмне забезпечення; аутентифікації, авторизації, бізнес-логіки тощо [13].

Об'єктами кіберзагроз є інфраструктура, веб-ресурси, користувачі, банкомати та POS-термінали, а останнім часом мобільні пристрої, IoT. Також постійно розширюється перелік сфер їх поширення, зокрема фінансова галузь, державне управління, сфери освіти, медицини, послуг, транспорту та зв'язку, роздрібної торгівлі, онлайн-сервіси, реальний сектор і оборонна промисловість, IT-сфера.

Аналіз тенденцій поширення кіберзагроз показав, що зростають атаки отримання даних, зокрема в I кварталі 2019 р. вони становили 54% від загальної кількості атак проти 19% і 48% в 2017 р. і IV кварталі 2018 р. відповідно. Найбільший інтерес викликають персональні (28%) та облікові (25%) дані, дані платіжних карток (16%), медична інформація та комерційна таємниця (по 9%).

Стосовно кібервійн – їх активність знаходиться в межах 1-2%. Значно зменшилась кількість атак задля отримання фінансової вигоди, адже, якщо в 2017 р. вони займали 73% від всієї кількості атак, то в І кварталі 2019 р. – це 30% (39% у IV кварталі 2018 р.). Водночас, майже вдвічі зріс хактивізм – 15% в І кварталі 2019 р. проти 7% у 2017 р. Найчастіше атаки спрямовані на державні (16%) і медичні (10%) установи, промислові підприємства (10%), а також фінансові та наукові установи, он-лайн сервіси, сфера послуг – по 6%. У структурі об'єктів активність кіберзагроз найбільш спрямована на інфраструктуру (58%), найменш – банкомати та POS-термінали, IoT (по 2%) [14].

Таблиця 2

Характеристика деяких видів кіберзагроз

Вид кіберзагрози	Характеристика
▪ таргетовані атаки (APT)	не мають масовий характер поширення, сплановані, цілеспрямовані атаки на конкретну компанію або державну установу задля доступу до корпоративної інформації з метою подальшої її монетизації
▪ кібервійни	комплекс ретельно спланованих і скоординованих суб'єктами міжнародних відносин кібератак деструктивного характеру на інформаційну інфраструктуру супротивника з метою послаблення позицій об'єкта впливу та досягнення політичних, економічних та військових цілей
▪ кібертероризм	терористична діяльність, що здійснюється у кіберпросторі або з його використанням; навмисна мотивована атака на інформацію, комп'ютерну систему або мережу, що спрямована на залякування та створення небезпеки для суспільства, провокування військового конфлікту
▪ хактивізм	субкультурний феномен, хакерський рух або ідеологія, що вже набула міжнародного масштабу, пропагує принципи «свободи слова» і «захисту прав людини» в кіберпросторі, проявом чого є кримінальна діяльність у різних проявах (політично мотивовані атаки на публічні сайти і поштові сервера, протести проти урядів, публікація конфіденційної інформації тощо) на технічних умовах анонімного використання комп'ютерів і глобальних мереж
▪ DDoS-атаки	1) на вхідний канал провайдера з метою забити його «паразитних» трафіком, блокуючи корисну інформацію («об'ємні» або Volumetric-атаки); 2) на мережеву інфраструктуру; 3) на сервер і операційну систему з метою використання ресурсів сервера; 4) на програмний додаток, коли сервіс перевантажується «сміттєвими» запитами, а легітимні запити залишаються без відповіді або вимагають значного часу на обробку
▪ апаратні закладки	зловмисні і спеціально замасковані модифікації електронних пристроїв для забезпечення прихованого доступу до обчислювальної техніки та мереж, зміни функціональності, зниження надійності, виведення з ладу, збору конфіденційної інформації
▪ акустичні атаки	через вбудовані динаміки або зовнішню акустику за допомогою звукових і ультразвукових хвиль викликають збій у роботі магнітних жорстких дисків під час читання та запису інформації, що може привести до програмних і апаратних несправностей у широкому спектрі пристроїв, як наслідок – втрата даних

Джерело: сформовано авторами на підставі опрацювання [13, 15, 16, 17, 18, 19, 20]

Цифрова економіка змінює суспільне життя, а її інноваційність відкриває нові можливості не тільки для економічного зростання країни,

конкурентоспроможності бізнесу, добробуту суспільства та якості життя окремих громадян, але вона також породжує нові мотиви та види кіберзагроз та противоправної діяльності.

Загальне розуміння незворотності поширення цифрової економіки прийшло зі стрімкою появою та формуванням ринку криптовалют, одночасно зі зростанням якого останні стали предметом і новою метою кіберзлочинців, що призвело до появи таких форм кіберзагроз: 1) кликджекінг (clickjacking) – введення до веб-сайтів шкідливого коду (невидимих елементів) для збору даних без згоди користувачів; криптоджекінг (cryptojacking) – скрипти для майнінгу криптовалюти за допомогою пристроїв відвідувачів сайту; 2) програми-вимагачі, що здійснюють прихований майнінг, використовуючи обчислювальні потужності чужих комп'ютерів для генерації криптовалюти, як наслідок – зниження продуктивності системи та завдання іншої значної шкоди, або агресивна атака, що шифрує файли, а за надання ключа дешифрування вимагається викуп у криптовалюті; 3) злом обмінників криптовалюти та криптовалютних бірж – наприклад неодноразові напади на новозеландський крипто-обмінник Cryptopia та однойменну біржу, втрати яких склали більше 16 млн дол. США або зламаний Coincchck з втратою 500 млн дол. США; 4) фішинг криптовалют – спам розсилка електронних листів від імені криптовалютних гаманців і бірж з метою крадіжки облікових даних персонального гаманця. Зокрема, в 2018 р. кількість фішинг-атак зросла на 350% [21].

Іншою технологією, яка зазнає руйнівного впливу є інтернет речей або IoT (Internet of things), кількість яких за прогнозами до 2025 р. збільшиться до 75 млрд пристроїв. Злом IoT здійснюється для майнінгу криптовалют, долучення до мереж DDos-атак тощо.

Поліаспектну природу відносно кіберзагроз має технологія штучного інтелекту (AI, Artificial intelligence), адже з одного боку використовується для ідентифікації та захисту від загроз, а з іншого – за її допомогою цілком ймовірно зросте обман користувачів соцмереж та ЗМІ, шантаж і вимагання. Серед перспективних AI-стартапів можна відмітити такі: 1) Darktrace – використовує машинне навчання для виявлення раніше невідомих кіберзагроз у режимі реального часу за принципами імунної системи людини; 2) Jask – автоматично виявляє загрози без залучення людських ресурсів; 3) Deep Instinct – розпізнає і попереджує загрози підвищеної стійкості завдяки складним алгоритмам навчання подібно здатності до навчання мозку людини; 4) Harvest.ай – алгоритми визначення «бізнес-цінності важливих документів, відслідковування їх використання та переміщення, розпізнавання і припинення витоку інформації внаслідок цілеспрямованої атаки або внутрішньої загрози до її копіювання або викрадення» [22].

Багато уваги приділяється вивченню можливостей технології блокчейн для забезпечення кібербезпеки, зокрема: захисту даних на основі децентралізованого сховища;

попередження DDos-атак за рахунок децентралізованого розподіленого збереження системи доменних імен (DNS); підвищення надійності транзакцій завдяки базовим принципам розподіленого реєстру, формування і контроль журналу їх історій; підвищення якості аутентифікації пристроїв і користувачів внаслідок усунення людського фактору.

Україна будує національну систему кібербезпеки. Передусім для протидії кіберзагрозам, запобіганню кіберризикам, боротьбі з кіберзлочинністю було сформовано інституційну інфраструктуру, яка включає Департамент кіберполіції, Ситуаційний центр забезпечення кібернетичної безпеки на базі Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України, Центр раннього виявлення та реагування на кібербезпеки при Державній службі спеціального зв'язку і захисту інформації. Напрацьовано концептуальний та нормативно-правовий базис (табл. 3).

Таблиця 3

Характеристика концептуальних документів України у сфері кібербезпеки

Концептуальний документ	Конкретизація змісту
Доктрина інформаційної безпеки України [23]	визначає національні інтереси в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері
Стратегія кібербезпеки України [24]	передбачає комплекс заходів, пріоритетів і напрямів забезпечення кібербезпеки, зокрема, створення і оперативну адаптацію державної політики, спрямованої на розвиток кіберпростору та досягнення сумісності з відповідними стандартами ЄС та НАТО
Закон України «Про основні засади забезпечення кібербезпеки України» [25]	визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки
Концепція розвитку цифрової економіки та суспільства України на 2018-2020 роки [26]	визначає першочергові кроки щодо імплементації відповідних стимулів та створення умов для цифровізації в реальному секторі економіки, суспільстві, освіті, медицині, екології тощо, виклики та інструменти розвитку цифрових інфраструктур, набуття громадянами цифрових компетенцій, а також визначає критичні сфери та проекти цифровізації країни.

Джерело: сформовано авторами за результатами опрацювання визначених джерел

Підкреслимо, що на початку 2019 р. розроблено програмні документи «Цифровий порядок денний України – 2020» і Національна стратегія Індустрії 4.0 – єдині програмні документи загальнонаціонального рівня, де зосереджено увагу на кібербезпеці у цифровому середовищі, надані конкретні пропозиції та рекомендації. Але вони не мають правової сили, адже Верховна Рада їх не розглянула до цього часу.

Також є необхідність розробки та впровадження національних стандартів у сфері кібербезпеки систем Індустрії 4.0. На жаль, в Україні, де зараз відбуваються бойові дії, у тому числі в кіберпросторі, дотепер відсутня Державна цільова програма із забезпечення кібербезпеки України, що дозволила б системно і комплексно координувати зусилля всіх органів державної влади у сфері забезпечення кібербезпеки.

З 2018 року Україна приєдналася до двоетапної оцінки Дорожньої карти інтеграції в Єдиний цифровий ринок ЄС, яку проводить Єврокомісія. В цьому напряму «найбільш важливими й актуальними напрямками цифровізації є кібербезпека, розвиток інновацій, електронного урядування та розвиток електронної торгівлі. У свою чергу це дозволяє розвинути українську цифрову інфраструктуру і ефективно поліпшити умови і якість життя людей» [27].

Отже, побудова цифрової економіки неможлива без розуміння технологічної і соціальної природи кіберзагроз, потребує ініціатив і дієвих кроків щодо розвитку і зміцнення інституційної та інформаційної інфраструктури на національному та глобальному рівнях, напрацювання надійної і несупере-чливої нормативно-правової бази, формування необхідних цифрових компетенцій і цифрової грамотності, у тому числі стосовно моделей кіберзагроз і механізмів кіберзлочинів та їх наслідків, дотримання принципів кібербезпеки в усіх сферах професійної діяльності та побудові смарт-орієнтованих екосистем тощо.

Список використаної літератури

1. Гуцалюк М.В. Оцінка реалізації стратегії кібербезпеки України з урахуванням досвіду європейських і світових практик. *Інформація і право.* 2019. № 2(29). С. 90-99.

2. Про основні засади забезпечення кібербезпеки України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення 11.02.2019).

3. National Military Strategy for Cyberspace Operations. URL: //www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf (accessed 15 Feb. 2019).

4. Cyber Security Strategy of the United Kingdom URL: http://ccpic.mai.gov.ro/docs/UK_cyber_security.pdf (accessed 15 Feb. 2019).

5. Estrategia de Ciberseguridad Nacional URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ES_NCSS.pdf (accessed 15 Feb. 2019).

6. National Cyber Security Strategy for Norway New national strategy for cybersecurity published by Norway URL:

https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf (accessed 15 Feb. 2019).

7. Rus I. Study of cybersecurity issues *Studia universitatis petru maior series oeconomica.* 2017. Vol. 1, P. 1-16.

8. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право.* 2012. № 2(5), С. 162-175.

9. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека». *Правова інформатика*. 2014. № 2(42), С. 54-62.

10. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity URL: https://www.iso27001security.com/html/27032.html (accessed 18 Feb. 2019).

11. Recommendation X.1205 (04/08) URL: https://www.itu.int/rec/T-REC-X.1205-200804-I (accessed 18 Feb. 2019).

12. Кибербезопасность. URL: http://digitalbusiness.by/napravleniya-sotrudnichestva/natsionalnyj-bank-respubliki-belarus/kiberbezopasnost (дата звернення 20.02.2019).

13. Кибератаки. Tadviser. URL: http://www.tadviser.ru/index.php (дата звернення 20.02.2019).

14. Актуальные киберугрозы. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-q1-2019/#id2 (дата звернення 21.02.2019).

15. Киберугрозы: статистика, практика и прогноз. URL: http://lib.itsec.ru/articles2/Oborandteh/kiberugrozy-statistika-praktika-i-prognoz (дата звернення 21.02.2019).

16. Современные киберугрозы – течение, развитие, прогноз. URL: http://www.cio-sibir.ru/files/Meet/2015/2015-10-09-03.pdf (дата звернення 21.02.2019).

17. Запорожець О.Ю. Кібервійна: концептуальний вимір. *Актуальні проблеми міжнародних відносин*. 2014. Вип. 121(ч. І), С. 80-86.

18. Топчій В.В. Кібертероризм в Україні: поняття та запобігання кримінально-правовими та кримінологічними засобами. URL: http://www.lj.kherson.ua/2015/pravo06/part_3/16.pdf (дата звернення 22.02.2019)

19. Буряк В.В. Цифровая экономика, хактивизм и кибербезопасность. Симферополь: ИП Зуева Т.В., 2019. 140 с.
20. Артамонова А.А. Аппаратные закладки как компонент вредоносного аппаратного обеспечения: обзор, классификация и анализ угрозы. *ИТпортал.* 2018. №1 (17). URL: http://itportal.ru/science/tech/apparatnye-zakladki-kak-komponent-v/ (дата звернення 22.02.2019).
21. Microsoft Security Intelligence Report URL: https://www.microsoft.com/security/blog/2019/02/28/microsoft-security-intelligence-report-volume-24-is-now-available/ (accessed 15 Feb. 2019).
22. 4 стартапа, которые создают искусственный интеллект для ведения кибервойн. URL: https://www.tsarev.biz/news/zapadnopartnerskij-kontrol-4-startapa-kotorye-sozdayut-iskusstvennyj-intellekt-dlya-vedeniya-kibervojn/ (дата звернення 21.02.2019).
23. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». URL: https://www.president.gov.ua/documents/472017-21374 (дата звернення 21.02.2019).
24. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». URL: https://zakon5.rada.gov.ua/laws/show/96/2016 (дата звернення 18.02.2019).
25. Про основні засади забезпечення кібербезпеки України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення 18.02.2019).
26. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації. URL: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80 (дата звернення 18.02.2019).
27. У МЕРТ пояснили, що є дієвим інструментом економічного зростання. URL: https://news.finance.ua/ua/news/-/444894/u-mert-poyasnyly-shho-ye-diyevym-instrumentom-ekonomichnogo-zrostannya (дата звернення 02.03.2019).