DOI https://doi.org/10.32405/2522-9931-2021-15(44)-221-232
УДК 007:316.77:341.326

Кириченко Микола Олексійович,
доктор філософії,
член-кореспондент Національної академії
вищої освіти України;
ректор ДЗВО «Університет менеджменту освіти».
Київ, Україна.
ORCID iD: https://orcid.org/0000-0003-1756-9140
kmoumo@gmail.com

БОРОТЬБА З УРАЗЛИВІСТЮ ЦИФРОВІЗАЦІЇ ЯК ДЕРЖАВНЕ ЗАВДАННЯ КОЖНОЇ КРАЇНИ

Анотація. У цій статті проаналізовано актуальну проблему, що зумовлена трансформаційними змінами сучасного світу в епоху цифрової глобалізації з прискореними темпами розвитку цифрових технологій. Автором зазначається, що ці зміни призводять до суттєвої уразливості цифровізації та загострюють необхідність інформаційної безпеки і кібербезпеки в країні. Аргументовано, що у процесі розвитку високих технологій виникло принципово нове середовище – кіберпростір, що формується із соціальної, технічної, телекомунікаційної, інформаційної, мережевокомп'ютерної складової частини. Кіберпростір одночасно виступає як суб'єкт та об'єкт впливу. Сучасна успішна геополітика неможлива без стійкого домінування у кіберпросторі. Акцентовано увагу на тому, що цифровізація в сучасних умовах є надзвичайно уразливою, бо є несанкціонований доступ до комп'ютерів, маються уразливості або лазівки у системі захисту, що дозволяють користувачеві (наприклад, системному адміністратору) обійти звичні заходи безпеки та отримати доступ до комп'ютера чи комп'ютерної системи. Зазначено, що з розвитком інформаційного суспільства керівники фірм, організацій та державних установ повинні проводити ефективні підходи до захисту цифрової інфраструктури. Її захист повинен стати основою стратегічного активу і пріоритетом державної безпеки, щоб такі мережі були неуразливі. Для цього у кожній компанії чи в цілому у державі слід відслідковувати стримування цих атак проти об'єктів власної інфраструктури та швидко відновлювати і вдосконалювати їх після будь-якого пошкодження. Підкреслюється важливість аналізу трансформацій сучасної кіберзлочинності, що потребує вивчення сценаріїв та перспектив розвитку інформаційного суспільства до 2030–2040 років,

https://doi.org/10.32405/2522-9931-2021-15(44)

стратегічного аналізу сценаріїв розвитку для України.

Ключові слова: цифровізація; інноваційне суспільство; кіберпростір; кіберзагрози; кібербезпека.

ВСТУП / INTRODUCTION

Постановка проблеми.

Четверта промислова революція («Industry 4.0») зумовила трансформаційні зміни сучасного світу, який живе в епоху цифрової глобалізації: безперервні потоки інформаційних даних, знань, ідей, інновації. Прискореними темпами в розвинених країнах розвиваються цифрові технології, де переважають технології «відкритих даних» (Open Data), «цифрові платформи» (Digital Platform), «блокчейн» (Blockchain) «цифрового робочого місця» (Digital Workplace), «багатоканальні інформування та залучення громадян» (Multichannel citizen engagement), «Інтернет послуги» (IoS), «Кіберфізичні системи» (Cyber-Physical System), «Смарт-факторія» (Smart Factory) тощо.

Масштаб і темп стрімких цифровізаційних процесів властивий і Україні, однак ці зміни призводять до суттєвої уразливості, що загострює необхідність інформаційної безпеки і кібербезпеки в країні.

Аналіз останніх досліджень і публікацій. Проблеми уразливості цифровізації, її наслідки для суспільства й держави, інформаційної безпеки і кібербезпеки є питаннями наукових досліджень зарубіжних вчених, зокрема, В. Гібсона, М. Гудмена, К. Шваба, Г. Шейна та інших. Серед вітчизняних науковців досліджуваній проблематиці та загрозам цифровізації приділяли увагу В. Бурячок, О. Вінник, С. Гнатюк, О. Голобородько, І. Гулівата, Ю. Грицюк, М. Камчатний, О. Климчук, З. Коваль, К. Краус, В. Ляшенко, І. Ніколіна, М. Руденко, Г. Почепцов, М. Присяжнюк, Н. Ткачук, Б. Толубко, В. Хорошко, Є. Цифра, С. Юрасов, С. Яремко та інші.

МЕТА ТА ЗАВДАННЯ / AIM AND TASKS

Мета статті полягає у концептуалізації значення проблеми боротьби з уразливістю цифровізації як державного завдання для кожної країни в епоху цифрової глобалізації та четвертої промислової революції («Industry 4.0»).

Відповідно до зазначеної мети у статті поставлено такі ***завдання***: розглянути зміст понять «цифровізація», «кіберпростір», «кіберзагрози», «кібербезпека», проаналізувати наявні дефініції, окреслити актуальні проблеми та можливі шляхи вирішення проблеми уразливості в процесі глобальної цифровізації.

https://doi.org/10.32405/2522-9931-2021-15(44)

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ / THE THEORETICAL BACKGROUNDS

Цифровізація – насичення фізичного світу електронно-цифровими пристроями, засобами, системами та налагодження електронно-комунікаційного обміну між ними, що фактично уможливлює інтегральну взаємодію віртуального та фізичного, тобто створює кіберфізичний простір [1].

Як зазначається в матеріалах проєкту «Цифрова адженда України – 2020» Мінекономрозвитку України, цифровізацію варто розглядати як інструмент, а не як самоціль. При системному державному підході «цифрові» технології будуть стимулювати розвиток відкритого інформаційного суспільства як одного з істотних факторів підвищення продуктивності, економічного зростання, створення робочих місць, а також покращення якості життя громадян України. Цифровізація для України носить позитивний соціальний характер, адже зосереджена на поліпшенні якості інфраструктури соціального забезпечення, якості соціальних послуг, організації прозорості та адресності соціальної допомоги, та скорочення витрат [2].

Разом з цим процес масштабної цифровізації усіх сфер життя призводить до того, що зростають кіберзагрози.

У міжнародному законодавстві й досі відсутнє єдине визначення понять: «кібернетична безпека», «кібернетична загроза», «кібернетичний захист», «кібернетичний простір», «кібернетична злочинність». Проблема кібербезпеки специфічна та глобальна, тому максимальна ефективність у боротьбі з новими загрозами може бути забезпечена, якщо міжнародні актори, приватні корпорації й асоціації об’єднають свої зусилля. Актуальність визначення змісту понять «кібербезпека» та «кіберзагроза» є важливим аргументом для покращення ефективності взаємодії на міжнародному рівні.

У процесі розвитку високих технологій виникло принципово нове середовище – ***кіберпростір,*** що формується із соціальної, технічної, телекомунікаційної, інформаційної, мережевокомп’ютерної складової частини. Кіберпростір одночасно виступає як суб’єкт та об’єкт впливу. Сучасна успішна геополітика не можлива без стійкого домінування у кіберпросторі.

Система кібернетичної безпеки (кібербезпеки) – сукупність узгоджених за завданнями елементів кібернетичної безпеки, які комплектуються та розгортаються за єдиним замислом і планом у кібернетичному просторі з метою забезпечення кібернетичної безпеки

https://doi.org/10.32405/2522-9931-2021-15(44)

інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем. Розвиток національної системи кібербезпеки має супроводжуватись відповідними корективами у процесі реформування сфери національної безпеки, а функціонування вказаної системи є неможливим без тісної співпраці з приватним сектором [3].

Кібернетичні загрози (кіберзагрози), як зазначається у Великому тлумачному словнику сучасної української мови, це наявні й/або потенційно можливі явища та чинники, що створюють небезпеку життєво важливим інтересам людини і громадянина, суспільства й держави, реалізація яких залежить від належного функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем [4].

Проєкт Стратегії забезпечення кібернетичної безпеки України визначає ***кібернетичну загрозу*** (кіберзагроза) як наявні й потенційно можливі явища та чинники, що створюють небезпеку інтересам людини, суспільства й держави через порушення доступності, повноти, цілісності, достовірності, автентичності режиму доступу до інформації, яка циркулює в критичних об'єктах національної інформаційної інфраструктури [5].

МЕТОДИ ДОСЛІДЖЕННЯ / RESEARCH METHODS

У процесі роботи нами використано такі методи дослідження: теоретикометодологічний аналіз наукових джерел, порівняльний аналіз теоретичних положень означеної проблеми ма метод інформаціоналізму.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ / RESEARCH RESULTS

Цифровізація в сучасних умовах є надзвичайно уразливою, так як має місце несанкціонований доступ до комп'ютерів, маються уразливості або лазівки у системі захисту, що дозволяють користувачеві (зокрема авторизованому, як-от системний адміністратор) обійти звичні заходи безпеки, наприклад, введення логіна і пароля користувача, та отримати доступ до комп'ютера чи комп'ютерної системи. Зламувач може використати такі шляхи доступу, щоб укріпитися на позиції в електронній мережі компанії або для багатьох інших цілей, в тому числі не завжди законних.

Все, що потребує зламувач, це вхід і цифровий плацдарм для проведення своїх шпигунських операцій. Більшість власників заражених комп'ютерів навіть гадки не мають, що за ними стежать хакери, а не виявлені користувачами недоліки комп'ютерної системи, відомі лише хакерам. Агентство купує інформацію про ці уразливості на тіньовому ринку у хакерів, які виявили їх, інколи сплачуючи по декілька тисяч доларів за кожну інформацію. Інколи платять компаніям – розробникам

https://doi.org/10.32405/2522-9931-2021-15(44)

програмного забезпечення та комп'ютерів за приховування інформації про вразливі місця або бекдори в їхніх продуктах, щоб агенство й хакери могли їх використовувати, інколи злочинці атакують незахищені інтелектуальні комунікаційні пристрої з різних міркувань, зокрема, з метою фінансового шахрайства [6, с. 367].

Проникаючи у такі комп'ютери, хакер зможе прочитати і скопіювати будь-які незашифровані документи, зокрема текстові файли, електронну пошту, аудіовізуальні файли, презентації, списки контактів і таке інше. Зашифровану інформацію прочитати важко, але можливо.

Зрештою одним із завдань таких організацій є зламування кодів. Китай – одна з найважливіших мішеней стеження та планування кібервійн, так як це країна зі стрімким технологічним розвитком, що робить також і її вразливою. США мають докази того, що Китай проникав у комп'ютерні мережі оборонних підрядників та інших американських компаній.

Едвард Сноуден, скандально відомий спеціаліст з ІТ-технологій, розповідав китайським журналістам, що США також зламували комп'ютери Пекінського університету Ціньхуа – одного з провідних освітніх і дослідницьких центрів країни державної комп'ютерної системи, що містить «інтернет-дані мільйонів китайських громадян». Можливо, це було однією з причин того, що Агенство національної безпеки США (далі – АНБ) теж прагнуло проникнути у цю систему. Едвард Сноуден назвав це зламування кодів масштабним, він показав журналістам документи, які свідчили про те, що в січні 2013 року АНБ проникло, принаймні, до 63 університетських комп'ютерів і серверів. За словами Сноудена, ці документи доводили втручання АНБ у певні комп'ютерні мережі та системи, позаяк містили IP-адреси, які могла отримати лише одна людина, яка мала фізичний доступ до комп'ютера.

Американські аналітики вважають, що китайські університети – це основний ресурс кадрів для уряду й органів влади. Китай – це найбільша мішень хакерів останніх років, однак не єдина, на яку вони націлені. Всі ці факти свідчать про те, що Інтернет в інформаційному суспільстві перетворюється на справжнє «поле битви» у неоголошених війнах. У рамках секретних програм агентства домовляються з технологічними компаніями щодо впровадження бекдорів у їхні комерційні продукти. У 2012 році Конгрес США виділив 250 млн. доларів на реалізацію цього продукту, відмічає у своїй праці Шейн Гарріс [7, с. 113]. Агентство отримало доступ до листування та розмов у Skype і до хмарного сховища Microsoft SkyDrive – і аналітики могли читати повідомлення користувачів іще до шифрування.

https://doi.org/10.32405/2522-9931-2021-15(44)

Експерти АНБ інсталюють у ці продукти вразливості, щоб згодом використати їх у шпигунських або кібервоєнних операціях, а за потреби вивести навіть з ладу технологічний продукт. Так, принцип дії «комп'ютерного хробака» Stuxnet, який знищив центрифуги на іранському ядерному виробництві, ґрунтується на невідомій раніше уразливості у системі управління компанії Siemens. Це також свідчить про те, що, можливо, виробник знав про цю вразливість і погодився її залишити, а потім АНБ використало інформацію про недоліки системи для створення «хробака» Stuxnet. Упродовж десяти останніх років АНБ спільно з британськими колегами з центру урядового зв'язку поклало чимало зусиль на боротьбу з криптографічними технологіями, інсталюючи приховані вразливості у поширенні стандартів шифрування.

Шифрування – це процедура перетворення даних (наприклад, електронного листа) в мішанину цифр і символів, які можна розшифрувати лише за допомогою ключа, яким володіє адресат. Бюджет американського агентства на підтримку кібербезпеки становить мільярди доларів США. Найуразливіші для нищівних кібератак саме такі об'єкти, як електростанції, підприємства атомної промисловості, газові трубопроводи, критично важливі об'єкти інфраструктури, а також банки й фінансові установи.

Коли компанія виявляє загрозу, відбувається «латання дір» і оновлення системи стає додатковим навантаженням, тим більше, що технологічна гнучкість різних компаній є різною. АНБ як військова й розвідувальна організація підтримує ринок кіберзброї, загрозливий для американських компаній в критично важливих об'єктах інфраструктури, проте позиціонує себе як озброєну орагнізацію, покликану захищати державу від зловмисників та їх атак. Агенство має власну виробничу базу, на якій працюють найкращі хакери США, більшість з яких зробила кар'єру в армії і навчалася на курсах із комп'ютерної освіти. США покладаються на вміння та знання цих фахівців, коли йдеться про кіберзмагання з Китаєм, який завжди матиме вагому перевагу за кількістю хакерів [7, с. 126].

Основу бізнесу компаній, що займаються кібератаками та кібершпигунством, становить обробка величезного обсягу інформації про незахищені комп'ютери, вразливість мереж із зазначенням їхнього програмного й апаратного забезпечення. Ботнет – це мережа комп'ютерів з таємно запущеним у них автономним програмним забезпеченням (ботами), яке дозволяє зловмисникам виконувати певні дії з використанням ресурсів інфікованого пристрою.

Наприклад, всесвітньо відома компанія Microsoft продовжує атакувати ботнети і її успіх надихає багатьох державних діячів та

https://doi.org/10.32405/2522-9931-2021-15(44)

керівників корпорацій, що співпраця між поліцією та корпоративними хакерами може бути дієздатним методом боротьби із кіберзлочинністю.

Тому, з розвитком інформаційного суспільства керівники фірм, організацій та державних установ повинні проводити ефективні підходи до захисту цифрової інфраструктури – мереж і комп'ютерів, від яких ми щодня залежимо. Захист цієї інфраструктури повинен стати основою стратегічного активу і пріоритетом державної безпеки, щоб такі мережі були безпечними, надійними і безвідмовними. Для цього в кожній компанії чи в цілому в державі слід відслідковувати стримування цих атак проти об'єктів своєї власної інфраструктури та швидко відновлювати і вдосконалювати їх після будь-якого пошкодження.

Захист кіберпростору повинен слугувати державним завданням кожної країни. Згідно із чинним законодавством в Україні відповідні міністерства повинні координувати політику кіберпбезпеки на рівні уряду, захищати комп'ютерні мережі цивільних державних служб і співпрацювати з компаніями заради захисту критично важливих об'єктів інфраструктури, під'єднаних до Інтернету пристроїв, контролю обладнання електростанцій, ядерних реакторів, банків та критично важливих інших інфраструктурних об'єктів.

Якщо аналітики виявили, що хакер намагається заразити комп'ютери, компанія може запрограмувати свої системи так, щоб заборонити виконання комп'ютерних програм з будь-яких USB-носіїв, інсталюючи захист, щоб опинитися у безпеці. Так, після атак на банківські сайти у 2012 році американські фінансові організації створили власні підрозділи стеження, в яких фахівці у сфері кібербезпеки вміють знаходити вразливості у програмному забезпеченні та мережевих конфігураціях, аналізувати шкідливе ПЗ, досліджувати методи його роботи й призначення, а також відбивати атаки.

Методи боротьби з уразливістю цифровізації, як державне завдання кожної країни, повинні розроблятися не лише на державному, а й приватному рівнях. Фундаментальне питання щодо нашого майбутнього у кіберпросторі полягає у тому, щоб ухвалити закони і правила, що регулюватимуть поведінку у ньому. Некеровані простори розпадаються, вони нездорові, вони дають прихисток злочинцям і терористам.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ / CONCLUSIONS AND PROSPECTS FOR FURTHER RESEARCH

Жодна держава не повинна розглядати своє майбутнє без відповідних антихакерських законів і правил. Вся дилема полягає у тому,

https://doi.org/10.32405/2522-9931-2021-15(44)

яку вагу ми надамо безпеці у кіберпросторі і хто за неї відповідатиме. Проте кіберпростір і надалі залишається колекцією приватних пристроїв і людство в інформаційному суспільстві дійшло до того, що почало залежати від нього, як від електрики чи водопостачання. Лише інформоване суспільство може підкорити громіздку військово-оборонну машину мирним цілям задля процвітання свободи і безпеки, сприяючи розвитку людського й соціального капіталу [8, с. 107–128].

Перспективи подальших досліджень. Підняті в статті проблеми не вичерпують всіх аспектів боротьби із кіберзлочинністю та уразливістю в цифровому суспільстві. У перспективі доцільним вважається зосередитися на вивченні нових складових кіберпростору, що формується із соціальної, технічної, телекомунікаційної, інформаційної, мережевокомп'ютерної та інших складових частин.

Інтерес також становить аналіз трансформації сучасної кіберзлочинності, що потребує вивчення сценаріїв та перспектив розвитку інформаційного суспільства до 2030–2040 років, стратегічного аналізу сценаріїв розвитку для України та формування відповідних інститутів і програм для протидії уразливості держави та особистості в ході подальшої цифровізації суспільства. Дослідження означених проблем і повинно стати предметом наступних наукових розвідок.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ / REFERENCES (TRANSLATED AND TRANSLITERATED)

[1] Верховна Рада України. (2018, Січ. 17). *Розпорядження № 67-р Кабінету Міністрів України «Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації».* [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#n13

[2] Цифрова адженда України – 2020. Концептуальні засади (версія 1.0), 2016, 90 с. [Електронний ресурс]. Доступно: https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf

[3] І. В. Діордіца, «Поняття та зміст національної системи кібербезпеки», *GOAL, Глобальна організація союзницького лідерства.* [Електронний ресурс]. Доступно: https://goal-int.org/ponyattya-ta-zmist-nacionalnoi-sistemi-kiberbezpeki/

[4] *Великий тлумачний словник сучасної української мови* / уклад. О. Єрошенко. Донецьк, Україна: ТОВ «Глорія Трейд», 2012, 864 с.

[5] *Стратегії забезпечення кібернетичної безпеки України. Проект*. [Електронний ресурс]. Доступно: https://niss.gov.ua/sites/default/files/2013-11/kiberstrateg.pdf

https://doi.org/10.32405/2522-9931-2021-15(44)

[6] М. Гудмен, *Злочини майбутнього: усе взаємопов'язане, усі вразливі і що ми можемо з цим зробити*; пер з англ. І. Мазарчук, Я. Машико. Київ, Україна: Вид-во Ранок: Фабула, 2019, 592 с.
[7] Г. Шейн, *Війн@: битви в кіберпросторі.* Київ, Україна: Ніка-Центр; Львів: Вид-во Анетти Антоненко, 2019, 296 с.
[8] М. Кириченко, «Вплив цифрових технологій на розвиток людського і соціального капіталу в умовах діджиталізованого суспільства», *Humanities studies: Collection of Scientific Papers*. Zaporizhzhia: ZNU, № 1(78), p. 107–128, 2019.

FIGHTING THE VULNERABILITY OF DIGITALIZATION AS A STATE OBJECTIVE OF EACH COUNTRY

Mykola Kyrychenko,
Habilitated Doctor in Philosophy,
Corresponding Member of National Academy of Sciences
of Higher Education of Ukraine;
rector of SIHE «University of Educational Management».
Kyiv, Ukraine.
ORCID iD: https://orcid.org/0000-0003-1756-9140
kmoumo@gmail.com

Abstract. This article analyzes the current problem caused by the transformational changes of the modern world in the era of digital globalization with the accelerated pace of digital technologies development. The author notes that these changes lead to a significant vulnerability of digitalization and highlights the need for information security and cybersecurity in the country. It is proved that in the process of high technology development cyberspace as a fundamentally new environment has emerged. It is formed from the social, technical, telecommunications, information, network and computer components. Cyberspace acts as both a subject and an object of influence. Modern successful geopolitics is impossible without stable dominance in cyberspace. Emphasis is placed on the fact that digitalization in modern environment is extremely vulnerable, as there is unauthorized access to computers, there are vulnerabilities or loopholes in the security system that allow the user (including an authorized, such as system administrator) to bypass the usual security measures and have access to a computer or computer system. It is noted that with the development of the information society, the heads of firms, organizations and government agencies must exercise effective approaches to the protection of digital

https://doi.org/10.32405/2522-9931-2021-15(44)

infrastructure. The protection of this infrastructure must be the basis of a strategic asset and a priority of national security for such networks to be secure. So each company or the state as a whole should monitor the deterrence of these attacks against its own infrastructure and quickly restore and improve it after any damage caused. The importance of the analysis of modern cybercrime transformations is underlined. It requires the study of scenarios and prospects for the development of information society until 2030-2040as well as strategic analysis of development scenarios for Ukraine.

Keywords: digitalization; innovation society; cyberspace; cyber threats; cybersecurity.

БОРЬБА С УЯЗВИМОСТЬЮ ЦИФРОВИЗАЦИИ КАК ГОСУДАРСТВЕННОЕ ЗАДАНИЕ КАЖДОЙ СТРАНЫ

Кириченко Николай Алексеевич,
доктор философии,
член-корреспондент Национальной академии
наук высшего образования Украины;
ректор ГУВО «Университет менеджмента образования».
Киев, Украина.
ORCID iD: https://orcid.org/0000-0003-1756-9140
kmoumo@gmail.com

Аннотация. В этой статье проанализирована актуальная проблема, обусловленная трансформационными изменениями современного мира в эпоху цифровой глобализации с ускоренными темпами развития цифровых технологий. Автором отмечается, что эти изменения приводят к существенной уязвимости цифровизации и обостряют необходимость информационной безопасности и кибербезопасности в стране. Аргументировано подчеркивается, что в процессе развития высоких технологий возникла принципиально новая среда – киберпространство, которая формируется по социальной, технической, телекоммуникационной, информационной, сетевой компьютерной составной части. Киберпространство одновременно выступает как субъект и объект воздействия. Современная успешная геополитика невозможна без устойчивого доминирования в киберпространстве. Акцентировано внимание на том, что цифровизация в современных условиях чрезвычайно уязвима, так как имеет место несанкционированный доступ к компьютерам, есть уязвимости или лазейки в системе

https://doi.org/10.32405/2522-9931-2021-15(44)

защиты, позволяющие пользователю (например, системному администратору) обойти привычные меры безопасности и получить доступ к компьютеру или компьютерной системе. Отмечено, что с развитием информационного общества руководители фирм, организаций и государственных учреждений должны использовать эффективные подходы к защите цифровой инфраструктуры. Ее защита должна стать основой стратегического актива и приоритетом государственной безопасности, чтобы такие сети были неуязвимыми. Для этого в каждой компании или в целом в государстве следует отслеживать сдерживания этих атак против объектов собственной инфраструктуры и быстро восстанавливать и совершенствовать их после любого повреждения. Подчеркивается важность анализа трансформаций современной киберпреступности, что требует изучения сценариев и перспектив развития информационного общества в 2030–2040 годы, стратегического анализа сценариев развития для Украины.

Ключевые слова: цифровизация; инновационное общество; киберпространство; киберугроза; кибербезопасность.

REFERENCES (TRANSLATED AND TRANSLITERATED)

[1] Verkhovna Rada Ukrainy. (2018, Sich. 17). Rozporiadzhennia № 67-r Kabinetu Ministriv Ukrainy «Pro skhvalennia Kontseptsii rozvytku tsyfrovoi ekonomiky ta suspilstva Ukrainy na 2018–2020 roky ta zatverdzhennia planu zakhodiv shchodo yii realizatsii». [Elektronnyi resurs]. Dostupno: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#n13

[2] Tsyfrova adzhenda Ukrainy – 2020. Kontseptualni zasady (versiia 1.0), 2016, 90 s. [Elektronnyi resurs]. Dostupno: https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf

[3] I. V. Diorditsa, «Poniattia ta zmist natsionalnoi systemy kiberbezpeky», GOAL, Hlobalna orhanizatsiia soiuznytskoho liderstva. [Elektronnyi resurs]. Dostupno: https://goal-int.org/ponyattya-ta-zmist-nacionalnoi-sistemi-kiberbezpeki/

[4] Velykyi tlumachnyi slovnyk suchasnoi ukrainskoi movy / uklad. O. Yeroshenko. Donetsk, Ukraina: TOV «Hloriia Treid», 2012, 864 s.

[5] Stratehii zabezpechennia kibernetychnoi bezpeky Ukrainy. Proekt. [Elektronnyi resurs].
Dostupno: https://niss.gov.ua/sites/default/files/2013-11/kiberstrateg.pdf

[6] M. Hudmen, Zlochyny maibutnoho: use vzaiemopoviazane, usi vrazlyvi i shcho my mozhemo z tsym zrobyty; per z anhl. I. Mazarchuk, Ya. Mashyko. Kyiv, Ukraina: Vyd-vo Ranok: Fabula, 2019, 592 s.

[7] H. Shein, Viin@: bytvy v kiberprostori. Kyiv, Ukraina: Nika-Tsentr; Lviv: Vyd-vo Anetty Antonenko, 2019, 296 s.

[8] M. Kyrychenko, «Vplyv tsyfrovykh tekhnolohii na rozvytok liudskoho i sotsialnoho kapitalu v umovakh didzhytalizovanoho suspilstva»,Humanities studies: Collection of Scientific Papers. Zaporizhzhia: ZNU, № 1(78), p. 107–128, 2019.

Стаття надійшла до редакції
12 січня 2021 року