Електронний журнал «Ефективна економіка» включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України № 975 від 11.07.2019). Спеціальності – 051, 071, 072, 073, 075, 076, 292.

Ефективна економіка. 2023. № 9.

DOI: http://doi.org/10.32702/2307-2105.2023.9.20
УДК 658.012.4

М. А. Міненко,
д. е. н., професор
ORCID ID: https://orcid.org/0000-0002-7492-3196
Л. М. Міненко,
д. філос. з іст. та археол.,
старший науковий співробітник, Національний університет оборони України
ORCID ID: https://orcid.org/0000-0003-0249-9856
А. О. Марченко,
к. т. н.,старший науковий співробітник,
Національний університет оборони України
ORCID ID: https://orcid.org/0000-0002-1268-8012
П. А. Марченко,
аспірант інституту аерокосмічних технологій,
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
ORCID ID: https://orcid.org/0009-0006-7261-6316

ДИГІТАЛІЗАЦІЯ В УМОВАХ ГЛОБАЛІЗАЦІЇ СВІТУ І ТОТАЛЬНОГО ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ

M. Minenko,
Doctor of Economics, Professor
L. Minenko,
PhD, Senior Researcher, National Defence University of Ukraine
A. Marchenko,
PhD in Technical Sciences, Senior Researcher,
National Defence University of Ukraine
P. Marchenko,
Postgraduate student of the Institute of Aerospace Technologies, National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute»

DIGITALISATION IN THE CONTEXT OF THE GLOBALISATION OF THE WORLD AND THE TOTAL USE OF DIGITAL TECHNOLOGIES

Приводом до написання означеної статті стала потреба науково-прикладного обґрунтування важливості застосування потенціалу дигіталізації для гарантування стійкості розбудови органів державної влади та військового управління, їх конкурентних й репутаційних переваг в умовах глобалізації світу і тотальної цифровізації. Заради досягнення сформованої мети використано абстрактно-логічний, діалектичний, аналізу та синтезу і графічний методи наукового дослідження. Обґрунтовано, що сьогодні й на перспективу ефективне функціонування будь-якої юридичної особи в Україні прямо залежить від усвідомлення того наскільки її керівництво цілеспрямоване використовувати ресурс дигіталізації заради налаштування технологічних процесів, процесів організування роботи, взаємозв'язків із заінтересованими сторонами. Зазначено, що через це потрібно володіти не лише знаннями і вмінням застосовувати відповідні інноваційні цифрові технології та мати їх у своєму розпорядженні, але й передбачати можливі наслідки від впливу шкідливих програмних засобів, а також розуміти важливість пропускної спроможності цифрових каналів. У зв'язку з цим, акцентовано увагу на необхідності внесення виважених змін і доповнень до змісту внутрішньо-організаційних (адміністративних) документів, які характеризують місце і роль складових базової системи адміністративного менеджменту, визначають впливовість загально-організаційної системи управління на продуктивність роботи органів державної влади та військового управління в цілому, кожного їх структурного підрозділу зокрема. Сформульовано авторський погляд на сутність понять «цифрові технології», «базова система адміністративного менеджменту», «інфокомунікаційна мережа», «інноваційно-цифрові технології», «потенціал цифрових технологій», «Індекс цифрової економіки та суспільства», «кібербезпека», «кіберзагроза», «шкідливі програмні продукти». У підсумку рекомендовано, що з метою обов'язкового унормування вищезазначеного, покрокові дії стосовно тотальної дигіталізації необхідно відобразити у Положенні «Про інформаційну політику юридичної особи», відповідним чином його погодити із заінтересованими сторонами, затвердити і забезпечити їх поетапну реалізацію. Вперше узагальнено перелік сучасних цифрових технологій, надано їх характеристики, а також різновидів шкідливого програмного забезпечення. Удосконалено науковий підхід до визначення і представлено, в авторському розумінні, поняття «цифрові

технології», «інфокомунікаційна мережа», «інноваційно-цифрові технології», «потенціал цифрових технологій», «Індекс цифрової економіки та суспільства», «кібербезпека», «кіберзагроза», «шкідливі програмні продукти». Набула подальшого розвитку прикладна вагомість дефініції поняття «базова система адміністративного менеджменту», необхідність її застосування у практичній діяльності, обов'язково використовуючи потенціал ресурсів всеосяжної цифровізації, з метою гарантування продуктивного впровадження управлінських новацій, у першу чергу, міжнародно визнаних стандартів і моделей ділової досконалості. Практична значущість представленої статті полягає у можливості комплексно оцінити широку палітру цифрових технологій, роль пропускної спроможності інфокомунікаційних мереж, ризики, що несуть шкідливі програмні продукти у разі нехтуванням вимог кібербезпеки, а головне, що стійкі конкурентні й репутаційні переваги органів державної влади та військового управління прямо залежать від можливості використати інноваційний інструментарій оцифрування на практиці, маючи в своєму штаті достатню кількість фахівців з якісним рівнем компетенцій у сфері дигіталізації, з метою гарантування дієвості впливу базової системи адміністративного менеджменту на ефективність функціонування загально-організаційної системи управління.

The reason for writing this article was the need for a scientific and applied substantiation of the importance of using the potential of digitalisation to ensure the sustainability of the development of public authorities and military administration, their competitive and reputational advantages in the context of globalisation and total digitalisation. In order to achieve this goal, the article uses abstract-logical, dialectical, analysis and synthesis, and graphical methods of scientific research. It is substantiated that today and in the future, the effective functioning of any legal entity in Ukraine directly depends on the awareness of the extent to which its management is committed to using the digitalisation resource to adjust technological processes, work organisation processes, and relationships with stakeholders. It is noted that this requires not only the knowledge and ability to apply relevant innovative digital technologies and have them at one's disposal, but also to anticipate the possible consequences of malware, and to understand the importance of digital channel capacity. In this regard, the author emphasises the need to make balanced changes

and additions to the content of internal organisational (administrative) documents which characterise the place and role of the components of the basic administrative management system, and determine the impact of the general organisational management system on the performance of public authorities and military administration in general, and each of their structural units in particular. The author's view on the essence of the concepts of «digital technologies», «basic system of administrative management», «information and communication network», «innovative digital technologies», «potential of digital technologies», «Index of digital economy and society», «cybersecurity», «cyber threat», «malicious software products» is formulated. As a result, it is recommended that in order to regulate the above, step-by-step actions regarding total digitalisation should be reflected in the Regulation «On the Information Policy of a Legal Entity», duly agreed with the stakeholders, approved and ensured their phased implementation. For the first time, the author summarises the list of modern digital technologies, provides their characteristics, and types of malware. The article improves the scientific approach to the definition and presents, in the author's understanding, the concepts of «digital technologies», «information and communication network», «innovative digital technologies», «potential of digital technologies», «Index of the digital economy and society», «cybersecurity», «cyber threat», «malicious software products». The applied significance of the definition of the concept of «basic administrative management system», the need for its application in practice, necessarily using the potential of the resources of comprehensive digitalisation, has been further developed in order to guarantee the productive implementation of managerial innovations, primarily internationally recognised standards and models of business excellence. The practical significance of the article lies in the ability to comprehensively assess the wide range of digital technologies, the role of information and communication network capacity, the risks posed by malicious software products in case of neglecting cybersecurity requirements, and most importantly, that the sustainable competitive and reputational advantages of public authorities and military administration directly depend on the ability to use innovative digitisation tools in practice, having a sufficient number of specialists with a qualitative level of competence in the field of digitalisation.

Ключові слова: *дигіталізація; цифрові технології; базова система адміністративного менеджменту; інфокомунікаційна мережа; Індекс цифрової економіки та суспільства; кібербезпека; шкідливі програмні продукти.*

Keywords: *digitalisation; digital technologies; basic administrative management system; information and communication network; Digital Economy and Society Index; cybersecurity; malicious software products.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Динамічна мінливість глобального світу і тотальна цифровізація, а також активний вплив, особливо, факторів зовнішнього середовища на поточну діяльність юридичних осіб та їх перспективу стійкої розбудови виступають головними умовами переосмислення реалій сьогодення й пошуку нових підходів до розв'язання завдань, пов'язаних з конкурентоспроможністю і набуттям якісного рівня репутаційних переваг. Це, у першу чергу, вимагає переоцінювання інструментарію впливу (примусу, спонукання), що використовують менеджери для спонукання підлеглих до продуктивної роботи, а також активно-тотального застосування нових інноваційних можливостей, які гарантуватимуть позитивне якісне виконання тактичних і стратегічних виробничих завдань. З огляду на це, в статті акцентовано увагу на тому, що необхідний потенціал мають засоби сучасної дигіталізації, зокрема, цифрові технології, адаптоване прикладання яких сприятиме оптимальній продуктивності роботи, раціональному використанню ресурсів, своєчасному досягненню наміченого. Водночас обґрунтовано, що одночасно потрібно приділяти належну увагу пропускній спроможності цифрових каналів, а головне – питанням кібербезпеки. За будь-яких обставин, для унормування задач щодо поетапної всеосяжної цифровізації, всі адміністративні наміри обов'язково повинні знайти своє відображення у змісті внутрішньо-організаційних (адміністративних) документів, які характеризують місце і роль кожної складової базової системи

адміністративного менеджменту органів державної влади та військового управління, й неодмінно підлягають виконанню.

Аналіз останніх досліджень і публікацій. У науковій літературі питання комплексно-прикладного застосування ресурсів дигіталізації з метою забезпечення належного рівня адміністрування діяльності органів державної влади та військового управління, підприємств (організацій, установ) різних форм власності (далі – юридична особа) не надається належної уваги. Водночас такі вчені й практики, як А. Халапсис [14], T. Ritter [30], P. Munteanu and L. Ciornei [27], J.-P. De Clerck [22], О. Гудзь, С. Федюнін, В. Щербина [4], K. Grünenberg, P. Mohl, K. O. Fog, and A. Simonsen [23], Г. Андрощук [1], Mahmood A., Akram T., Chen H.F., Chen S.G. [26], V. Rebenok, R. Al-Namri, O. Butko, V. Fedorenko, O. Tereshchenko, N. Tsimokh [29], Д. Чернишев, Д. Рижаков, О. Хоменко, С. Петруха, О. Кучеренко, М. Горбач [15] та інші в своїх працях характеризують поняття дигіталізації та її складових, а також досліджують питання використання цифрових та інфокомунікаційних технологій, які доцільно використовувати для підвищення ефективності й продуктивності роботи юридичних осіб. Разом з тим, у статті науковців М. А. Міненка та В. А. Піддубного [10] охарактеризовано зміст елементів і підсистем базової системи адміністративного менеджменту, проте не зазначено роль дигіталізації заради забезпечення її дієвості з метою гарантування ефективності загально-організаційної системи управління. Крім того, Г. Андрощук [2], окремо, з’ясовує значення Індексу цифрової економіки і суспільства. Такий підхід може бути використаний для оцінювання ефективності органів державної влади (військового управління), підприємств (організацій, установ) різних форм власності нашої держави. В Україні застосування дигіталізації було унормоване окремими Указами Президента та законодавчими актами держави [12; 13]. Як наслідок, звертаючи увагу на актуальності цього наукового напряму, запропоновано авторське бачення стосовно системного використання ресурсів дигіталізації в щоденній діяльності

юридичних осіб, зважаючи на пропускні можливості інфокомунікаційної мережі та негативний вплив шкідливих програмних продуктів.

Формулювання цілей статті (постановка завдання) полягає в обґрунтуванні доцільності поетапно-всеосяжного застосування широкої палітри ресурсів дигіталізації для покращення дієвої впливовості базової системи адміністративного менеджменту на ефективність функціонування загально-організаційної системи управління, продуктивність роботи кожного структурного підрозділу і штатного працівника органів державної влади та військового управління, стійкість їх конкурентних і репутаційних переваг в умовах насичено-глобалізованого, динамічно-мінливого світу й тотальної цифровізації.

Виклад основного матеріалу дослідження. Виклики, що виникають в сучасних умовах кризових станів, пов’язані з потребою у швидкому отриманні та стабілізації конкурентних і репутаційних переваг, а також оперативному адаптуванні механізму організування виробничих процесів до впливу внутрішніх й зовнішніх факторів соціально-економічного та суспільно-політичного середовища (як прямої, так і непрямої дії). Це дедалі частіше спонукає керівників органів державної влади та військового управління (далі, юридичної особи) до переходу на якісно новий інноваційний рівень використання інструментарію адміністрування. Так, дійсно, в умовах глобалізації світу і тотальної цифровізації, традиційні підходи щодо формування базової системи адміністративного менеджменту [10], як підґрунтя для налаштування необхідної дієвості його загально-організаційної системи управління, впровадження та ефективного застосування управлінських новацій з метою набуття належного стану ділової досконалості, без використання ресурсу дигіталізації та, безпосередньо, модерних цифрових технологій, вже не можуть гарантувати стійкий розвиток будь-якої юридичної особи, а часом не спроможні навіть забезпечити стабільну роботу на вже досягнутому рівні.

Зважаючи на це, та для більш змістовного усвідомлення місця і ролі означеного, а головне, з урахуванням однієї з важливих нинішніх вимог

стосовно гарантування ефективності функціонування органів державної влади та військового управління у глобальних світових умовах і середовищі тотальної цифровізації, маємо констатувати, що дефініція «digital» є похідною від латинського «digitalis» (у перекладі − «цифри») [25]. З іншого боку, термін «дигіталізація» походить від англійського «digitalization» (у перекладі – «оцифровування», «цифровізація», «приведення до цифрової форми»). Разом із тим, окремі науковці пропонують більш ширше трактування дигіталізації, ніж те, що це є «певним шляхом погодження будь-якої інформації з цифровою формою» (табл. 1).

Таблиця 1. Окремі визначення терміну «дигіталізація»

Науковці (джерела)	Визначення терміну «дигіталізація»
Халапсіс О. В.	це пов'язаний із тенденцією приведення в електронний вигляд найрізноманітніших видів використовуваної людиною інформації процес «оцифровування буття» [14].
Brennen S.	це запровадження або збільшення використання організаціями, в певній галузі, країні тощо цифрових і комп'ютерних технологій [30].
Ж.-П. де Клерк	це використання цифрових даних, відокремлених від фізичних носіїв, для автоматизації робочих і бізнес-процесів [22].
Оксфордський словник англійської мови	це дія або процес з оцифровування, перетворення аналогових даних (зображень, відео- та текстових матеріалів) у цифрову форму [28].
Гудзь О. Є., Федюнін С. А., Щербина В. В.	це заснований на можливостях сучасної ІТ-індустрії процес застосування підприємствами сучасних інформаційно-комунікаційних технологій для досягнення своєї мети, зорієнтований на трансформацію існуючих бізнес-процесів шляхом їх диджиталізації [4].

Джерело: розроблено авторами за результатами дослідження.

Натомість, на нашу думку, цифрові технології (англ. – «Digital technology») – це системи, що базуються на універсальних методах кодування та передачі інформації в дискретному форматі (сигнал поширюється через дискретні полоси аналогових рівнів, а не у вигляді неперервного спектру), що дають змогу використовувати електронні інструменти, пристрої і програмні ресурси для обробки, генерації та зберігання даних, а також – передачі (обміну між абонентами) у найкоротші строки (сформовано авторами за результатами дослідження). Сьогодні, успішні практики визначають і рекомендують перелік

цифрових технологій, які доцільно використовувати на нинішньому етапі розвитку глобального світу й у середовищі тотальної цифровізації, а саме: хмарні та мобільні, блокчейн, віртуалізації, ідентифікації, штучного інтелекту, біометричні, доповненої реальності, адитивні (3D-друк) тощо (табл. 2).

Таблиця 2. Можливі варіанти цифрових технологій

Назви цифрових технологій	**Коротка характеристика**
Хмарні технології	це технології розподіленої обробки цифрових даних, за допомогою яких комп'ютерні ресурси надаються інтернет-користувачеві як онлайн-сервіс. За таких умов, всі необхідні для роботи програми та їхні дані знаходяться на віддаленому інтернет-сервері й тимчасово зберігаються (кешуються) на клієнтській стороні. Перевага полягає в тому, що користувач має доступ до власних даних, але не повинен піклуватися про периферію, операційну систему і програмне забезпечення, з яким він працює [21].
Технології «Великих даних» (англ. «Big Data»)	це сукупність інструментів, процедур і методів обробки як структурованих, так і неструктурованих цифрових даних величезних обсягів й значного їх різноманіття для отримання результатів з метою подальшого використання. Основними ознаками «Великих даних» є «три V»: «обсяг» (volume) – величина фізичного обсягу; «швидкість» (velocity) – швидкість накопичення, необхідність високошвидкісної обробки та отримання результатів; «різноманіття» (variety) – можливість одночасної обробки різних типів структурованих і неструктурованих даних [21].
Мобільні технології	це технології, які використовуються окремо або сукупно з іншими інформаційними та комунікаційними технологіями, для зручної роботи з портативними цифровими мобільними пристроями (смартфонами, планшетними комп'ютерами, електронними книгами), що дозволяє здійснювати операції з отримання, обробки, використання та поширення інформації [16].
Блокчейн технології	це архітектура зберігання інформації таким чином, що забезпечує незмінність історичних даних, а фактично, сформований децентралізований і розподілений реєстр у мережевій інфраструктурі, який використовується для накопичення, використання та передачі інформації [17].
Технології віртуалізації	це процеси об'єднання різних обчислювальних ресурсів та їх подальше перенесення з фізичної обчислювальної машини на віртуальну, а по суті, технологія, що дозволяє симулювати апаратну частину обчислювальних потужностей для створення програмних сервісів [6]. Віртуалізація буває серверна (емуляція (імітація) роботи апаратної частини серверів), застосунків (прикладна програма або додаток), робочих столів, мережева і систем зберігання даних. Дані типи віртуалізації можна використовувати як окремо, так і комбінувати з необхідною ефективністю [11].

Назви цифрових технологій	Коротка характеристика
Технології ідентифікації (від лат. Identifico – ототожнювати)	це певні дії щодо розпізнавання користувача в інформаційній системі, як правило, за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається цією системою. Ідентифікація дозволяє користувачу повідомити своє ім'я за допомогою унікального електронного параметра – ідентифікатора, який є відомим іншій стороні. Під час ідентифікації здійснюється порівняння заявленого користувачем параметра на відповідність відомому іншій стороні. В разі успішної ідентифікації відбувається автентифікація. Шляхом автентифікації інша сторона переконується, що користувач саме той за кого він себе видає (використовується пароль, у випадку парольної автентифікації, або інший секретний параметр) [7].
Технології штучного інтелекту (англ. Artificial intelligence)	це набір технологій, які дозволяють комп'ютеру виконувати різні функції, притаманні людині, наприклад: «Google Deep Mind» (аналізує інформацію, планує дії без участі людини, володіє «уявою»); «Google Clips» (оптимізовує процес фотографування без участі людини); «ChatGPT» (нейромережа-трансформер, яка вміє генерувати і редагувати тексти, відповідати на запитання, здійснювати семантичний пошук і створювати стислий виклад змісту тексту); алгоритм «Brain» (використовує YouTube для рекомендації контенту); безпілотні автомобілі «Google», «Uber», «Tesla» (сучасні засоби пересування, які можуть функціонувати завдяки використанню датчиків, камер, радарів і штучного інтелекту). По суті, це здатність машин симулювати розум та імітувати людські когнітивні здібності, тобто, збирати й адаптувати зовнішні дані, а на їх основі навчатися ухвалювати рішення і робити висновки, як могла б людина [5].
Біометричні технології	це можливість швидкої і простої ідентифікації або аутентифікації (верифікації) без спричинення якихось незручностей індивідуумові, тобто, використання унікальних вимірювальних параметрів людини для її ідентифікації (ототожнення) та верифікації (підтвердження) [23].
Технології доповненої реальності (англ. augmented reality або AR)	це доповнення фізичного світу за допомогою цифрових даних, яке забезпечується комп'ютерними пристроями (смартфонами, планшетами або ж окулярами AR) в режимі реального часу. Доповнена реальність є складовою змішаної реальності (англ. mixed reality) і є поєднанням реального світу з віртуальним: відбувається накладання на середовище навколо нас певної частинки віртуальної інформації, наприклад, графіку, звуків, анімації тощо [18].
Адитивні технології (технології пошарового синтезу)	це одна з форм технологій адитивного виробництва, де тривимірний об'єкт створюється шляхом накладання послідовних шарів матеріалу (друку, вирощування) за даними цифрової віртуальної 3D моделі спеціальним пристроєм – 3D-принтером, який пропонує розробникам продуктів можливість друку деталей і механізмів з декількох матеріалів та з різними механічними і фізичними властивостями за один процес складання [26] .

Назви цифрових технологій	Коротка характеристика
Інформаційно-комунікаційні технології	це неперервний зв'язок інформаційних і телекомунікаційних елементів інформаційного обміну, які розвиваються в процесі конвергенції (взаємного проникнення), що характеризує об'єднання телекомунікацій з інформаційними, комп'ютерними й радіотехнологіями, використання яких забезпечує доставлення сигналів електрозв'язку від джерел до споживачів, із можливістю ідентифікації їх інформаційного змісту та застосування оптимальних методів обробки, включаючи методи передавання, маршрутизації, перетворення, програмування [29]; результат інтелектуальної діяльності, сукупність систематизованих наукових знань, технічних, організаційних та інших рішень про перелік та послідовність виконання операцій для збирання, обробки, накопичення та використання інформаційної продукції, надання інформаційних послуг [12].

Джерело: розроблено авторами за результатами дослідження.

У будь-якому випадку, практичний досвід діяльності державних і громадських інституцій, а також органів військового управління провідних країн світу, свідчить, що наведені в таблиці 2 цифрові технології, як головні складові всеосяжної дигіталізації, допомагають: створити якісно-новий механізм вироблення, ухвалення і реалізації адміністративних рішень (оперативних, поточних, стратегічних); налагодити ефективну взаємодію із заінтересованими сторонами; перевести процеси організування роботи на новий якісно-технологічний рівень надання послуг; підвищити продуктивність праці та результативність роботи; прискорити надання послуг; стабілізувати конкурентні та репутаційні переваги. Фактично, дигіталізація передбачає кардинальну зміну механізмів і методів управління та вимагає модифікації мислення менеджерів, їх стилю керівництва, та підходів до налаштування і використання підсистем планування, бюджетування, ресурсного забезпечення роботи. Крім того, дигіталізація впливає на організування, супровід, контролювання, регулювання і мотивування діяльності штатного персоналу [4]. Це переконує в тому, що все вище наведене безпосередньо пов'язано з об'єктивною доцільністю внесення змін до внутрішньо-організаційних (адміністративних) документів, які характеризують місце, роль і змістовність, у першу чергу, елементів й підсистем базової системи адміністративного

менеджменту, а також регламентують специфіку функціонування загально-організаційної системи управління органів державної влади та військового управління в цілому, кожного структурного підрозділу і штатного працівника зокрема. Тобто, застосування інструментарію цифровізації передбачає необхідність перегляду внутрішніх нормативних документів адміністрацією (апаратом управління) (починаючи зі Статуту або Положення про організування роботи). В цьому контексті можуть знадобитися корективи і перезатвердження цих документів відповідно до встановленого порядку, з урахуванням адміністративного впливу, статусу й взаємозв'язків по вертикалі та по горизонталі управління, зокрема, з основними заінтересованими сторонами (стейкхолдерами). Відповідно, стає вагомішим практичне значення дефініції поняття «базова система адміністративного менеджменту». За таких умов, базова система адміністративного менеджменту є комплексом відносно відокремлених, водночас, взаємозалежних елементів, що через налагоджені наскрізні підсистеми комунікацій із заінтересованими сторонами, діловодства і документування діяльності, затверджені статут, штатний розпис, організаційну структуру управління, правила внутрішнього трудового розпорядку, положення про структурні підрозділи і посадові (робочі) інструкції (контракти, трудові договори (угоди)), визначені виробничі завдання, шляхом реалізації функцій адміністративного менеджменту, використовуючи необхідний ресурсний потенціал (у тому числі інструментарій тотальної дигіталізації), забезпечують досягнення сформованої мети (цілей), яка(які) відповідає(ють) місії (цінностям, візії, баченню, політиці) та обраній стратегії(ям) розвитку, не суперечать нормам колективного договору і кодексу корпоративної етики, законам, принципам і методам управління, а також сприяють процесу сертифікації й дотриманню норм стандартів (регламентів), що встановлюють цілеспрямовано-дієві умови роботи у відповідному соціально-економічному і суспільно-політичному зовнішньому середовищі та є основою для формування належного рівня ділової досконалості, гарантуючи результативне функціонування загально-організаційної системи управління і конкурентоспроможну стійкість

та репутаційні переваги будь-якої юридичної особи в умовах насичено-глобалізованого і динамічно-мінливого світу й суцільної цифровізації (сформовано авторами за результатами дослідження з використанням [10].

Крім того, щоб гарантувати оптимальну продуктивність і результативність роботи у нових умовах загальної цифровізації глобального світу будь-якому органу державної влади та військового управління необхідно розробляти і реалізовувати нові послуги, не тільки використовуючи широке різноманіття і потенціал інноваційних цифрових технологій, але й пропускну спроможність інфокомунікаційної мережі зі всіма заінтересованими сторонами. Адже, по суті, інфокомунікаційна мережа – це комплекс технічних засобів, зокрема, мережевих ресурсів (термінальних пристроїв користувачів, кінцевих систем мережі (хостів) та універсальної платформи виробництва й надання послуг, які відповідають різноманітним вимогам абонентів до їх типу та якості), призначених для спільної участі у виробництві й наданні телекомунікаційних, інформативних та інших послуг інформаційного співтовариства, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень і звуків або повідомлень за допомогою радіоканалів, а також – проводових, оптичних чи інших електромагнітних систем між кінцевим обладнанням, а фактично, перенесення в просторі інформативних повідомлень і взаємодію комунікаційних систем, виробництво нових послуг та інформації (сформовано авторами за результатами дослідження з використанням [24]). Саме такий стратегічно виважений підхід до адаптовано-раціонального і комплексного використання потенціалу дигіталізації гарантуватиме стійкі конкурентні позиції на прогнозований період, сприятиме покращенню репутації органів державної влади та військового управління.

Отже, маємо констатувати, що дієвість роботи будь-якої юридичної особи гарантується не лише завдяки впровадженню управлінських новацій але й прямо залежить від інноваційно-цифрових технологій та продуктивності інфокомунікаційної мережі, яку адаптовано-оптимально використано для налаштування, супроводу та отримання необхідних кінцевих результатів як за

рахунок модернізації базової системи адміністративного менеджменту загалом, так і кожного елемента загально-організаційної системи управління зокрема. З метою більш об’єктивного усвідомлення корисності таких кроків варто пам’ятати, що інноваційно-цифрові технології – це новітні, засновані на універсальних методах кодування і передачі інформації, дискретні системи, що, на відміну від вже існуючих, дозволяють за допомогою нових (модернізованих) електронних інструментів, пристроїв і програмних ресурсів здійснювати значно швидше за часом та якісніше за змістом обробку, генерування або зберігання даних (сформовано авторами за результатами дослідження).

Крім того, важливого значення набуває відсоток покриття оцифруванням виробничого простору органів державної влади та військового управління. Тому, для максимального прикладного ефекту, дигіталізацією має бути охоплений увесь технологічний ланцюг процесів організування роботи з надання послуг. Проте, чим досконало-системніше буде застосоване оцифрування і продуктивніше налагоджені цифрові канали, тим адаптовано-гарантованішими будуть перспективи стійкого конкурентного й репутаційного розвитку. Натомість, для впровадження необхідно обирати цифрові технології з відповідним потенціалом можливостей, виходячи з міркувань, що потенціал цифрових технологій – це сукупність наявних та/або скритих можливостей (наприклад, запасу пропускної спроможності, продуктивності) дискретних систем, заснованих на універсальних методах кодування і передачі інформації, що гарантують, за допомогою електронних інструментів, пристроїв і програмних ресурсів, здійснення обробки, генерування або зберігання даних, а також їхню якісну передачу (обмін між абонентами) у найкоротші проміжки часу, які задовольнятимуть споживачів певного функціонального спрямування, виробничого ланцюга, сфери діяльності (сформовано авторами за результатами дослідження).

Проте, маємо констатувати, що процеси впровадження тотальної дигіталізації відбуваються не достатньо динамічно. Зокрема, 19 червня 2020 року Європейська комісія (ЄК) опублікувала Індекс цифрової економіки

та суспільства 2020 (Digital Economy and Society Index 2020 (DESI 2020)), що передбачає оцінювання п’яти факторів: можливості підключення (розширення фіксованої і мобільної широкосмугової інфраструктури, швидкості й доступності); кадрові ресурси (цифрова грамотність населення); використання Інтернету для спілкування або здійснення транзакцій; інтеграція цифрових технологій (частка цифрового контенту, використання цифрових технологій, застосування електронної комерції); цифрові публічні послуги (розвиток і використання електронних державних служб) [15]. Практично, Індекс цифрової економіки та суспільства – це зведений індекс, який узагальнює відповідні показники ефективності цифрових технологій в Європі й відстежує еволюцію держав-членів Європейського Союзу (ЄС) в сфері цифрової конкурентоспроможності, тобто, вимірює і порівнює прогрес країн ЄС в царині цифрової економіки та засвідчує користь цифровізації для суспільства (сформовано авторами за результатами дослідження). Метою його публікації є встановлення прогресу стосовно досягненні цілей цифрової економіки в ЄС і моніторинг стану цифрового розвитку окремих держав-членів [1]. Звіт дає змогу виявити пріоритетні напрями цифрової економіки держав-членів ЄС, що вже сьогодні вимагають конкретних дій та інвестицій. Разом із тим, для порівняння з країнами за межами єврозони, був розроблений Міжнародний індекс цифрової економіки та суспільства (I-DESI), який має на меті віддзеркалити і розширити Європейський індекс цифрової економіки та суспільства (DESI) шляхом виявлення індикаторів, що вимірюють аналогічні змінні для країн не членів ЄС.

Наразі, результати розрахунку окреслених індексів свідчать, що за 2019 рік у всіх державах-членах ЄС досить повільно зростає рівень оцифровування. Попри все, лідерами стали: Фінляндія, Швеція і Данія. Останні місця в рейтингу зайняли: Румунія, Греція, Болгарія. Чотири найбільш прогресуючі в питаннях дигіталізації держави-члени ЄС (Фінляндія, Швеція, Нідерланди, Данія) перебувають у рейтингу країн світу після Південної Кореї, за якими слідують Японія і США. Водночас, дані про інтеграцію цифрових технологій до

базової системи адміністративного менеджменту, загально-організаційних систем управління і виробничих процесів юридичних осіб значно різняться залежно від розміру компаній, сектора економіки, до якого вони належать, і держави, що юридично, фіскально і геополітично впливає на їхню діяльність. Так, у 2019 році 38,5% великих виробників покладалися на сучасні сервіси хмарних технологічних обчислень, а 32,7% використовували технологічні рішення «Великих даних». Натомість, переважна більшість малих і середніх підприємств (МСП) користувалися хмарними сервісами і 12% – технологіями «Великих даних» (тільки 17,5% МСП реалізували власну продукцію онлайн, що на 1,4% більше порівняно з 2016 роком)) [1]. Фактично, це демонструє, що юридичні особи, навіть, розвинених країн світу, маючи достатні ресурси, не можуть використати весь потенціал цифрових технологій власної держави. Варто констатувати, що в сфері цифровізації Україна значно відстає, застосовуючи близько 3% власних можливостей до оцифрування.

Паралельно з впровадженням цифрових технологій, переважна кількість юридичних осіб, формуючи базові системи адміністративного менеджменту з метою налагодження ефективності функціонування загально-організаційних систем управління, що гарантуватимуть продуктивність роботи кожного штатного працівника, структурного підрозділу і юридичної особи загалом, надзвичайно активно і фахово почали перейматися проблемами кібербезпеки (ІТ-безпеки). Сутнісно, кібербезпека – це стан охорони життєво важливих інтересів окремих фізичних та юридичних осіб, суспільства, держави і країни загалом у середовищі, яке виникає внаслідок функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, шляхом напрацювання комплексу практичних порад і технологічно-обґрунтованих рішень, практична реалізація яких допомагає захистити означені системи, інфокомунікаційну мережу (digital-канали), а також інформаційні електронні ресурси (дані) від несанкціонованого доступу зовні (кібератак), що гарантує своєчасне виявлення, запобігання і нейтралізацію реальних й потенційних загроз у кіберпросторі для фізичних та юридичних осіб, національній безпеці

України загалом, а у підсумку – стійкий розвиток інформаційного суспільства та цифрового комунікативного середовища (сформовано авторами за результатами дослідження з використанням [13]). Водночас, кіберзагроза – це наявні й потенційно можливі явища та чинники, викликані протиправними діями суб'єктів інформаційних правовідносин, які створюють небезпеку важливим інтересам фізичних та\або юридичних осіб, суспільства, держави, країни в цілому щодо можливості формування, збирання, одержання, зберігання, використання, поширення, захисту інформації через порушення її доступності, повноти, цілісності, достовірності, автентичності режиму доступу (сформовано авторами за результатами дослідження з використанням [13]). Сучасна актуальність цих питань пояснюється тим, що, останніми роками, на дієвість функціонування юридичних і фізичних осіб та, особливо, органів державної влади та військового управління, які для підвищення своєї продуктивності використовують цифрові технології і мережу digital-каналів, мають значний вплив комп'ютерні віруси, хробаки, трояни, поштовий спам, фішингові повідомлення, DDoS-атаки і програми-вимагачі (Ransomware) (табл. 3).

Таблиця 3. Різновиди шкідливих програмних продуктів

Назва шкідливого програмного продукту	**Коротка характеристика**
Комп'ютерні віруси	це різновид шкідливого програмного забезпечення, що здатне поширювати власні вірусні електронні копії з метою інфікування і пошкодження даних на пристрої жертви із вже інших інфікованих пристроїв, через носії інформації (CD, DVD тощо) або Інтернет-мережу. По суті, це спеціальний код, який несе загрозу для комп'ютера, через що може на ньому пошкодити або видалити файли і навіть програми. Віруси не завжди пошкоджують файли, жорсткі диски або комп'ютери. Зазвичай, вони впливають на продуктивність (інфікований комп'ютер має починає «гальмувати») і стійкість системи. Щоб вірус міг «заразити» комп'ютер або почати поширюватися, достатньо виконати будь-яку дію (наприклад, відкрити інфіковане вкладення електронної пошти). Некоректно написаний вірус може заповнити жорсткий диск комп'ютера так, що його необхідно буде повністю переформатовувати [29; 8].

Назва шкідливого програмного продукту	**Коротка характеристика**
Комп’ютерні трояни	це різновид шкідливого програмного забезпечення, яке прикриває негативну мету свого призначення за допомогою відповідного електронного маскування всередині іншої програми, проте, на відміну від комп’ютерного вірусу, нездатне поширюватися (відтворювати себе) самостійно, у зв’язку з чим на пристрій користувача-жертви потрапляє через приховане завантаження спеціальним кодом або методами соціальної інженерії, використання існуючих вразливостей (за допомогою комп'ютерних вірусів, мережевих або поштових хробаків, програмного забезпечення). Після того як комп’ютерний троян потрапив до операційної системи він дозволяє комп’ютерному злочинцю (хакеру) отримати доступ до інформації, що зберігається на інфікованому комп'ютері. Троянська програма досить часто використовується для викрадення і передавання паролів, логінів, номерів кредитних карт, іншої конфіденційної інформації [29; 8].
Комп’ютерні хробаки	це різновид шкідливого програмного забезпечення, код якого поширюється незалежно від бажання користувача і дуже схожий на комп’ютерний вірус. Зазвичай, може подолати всі етапи розповсюдження самостійно (мережевий хробак) або використовує агента-користувача тільки на 2-му етапі (поштовий хробак). Застосовує адреси для розсилки інфікованих електронних повідомлень і часто вживає або підробляє їх в наступних електронних повідомленнях, щоб ці інфіковані повідомлення виглядали досить правдоподібно. Здатний до самовідтворення і поширюється не лише по всьому комп’ютеру але й автоматично розсилає свої копії електронною поштою. Поширюючись по мережах, може перевантажувати канали зв'язку, створюючи несанкціонований трафік. Різке зростання несанкціонованого трафіку призводить до перевантаження або відмови у роботі. Хробаки не завжди пошкоджують комп'ютери, проте, викликають істотне зниження продуктивності комп'ютера і мережі, а також їх нестабільність [29; 9; 3].
Поштовий спам	це небажані повідомлення у будь-якій формі, найчастіше електронні листи (чати), надіслані на велику кількість адрес через Інтернет-мережу, соціальні медіа або навіть голосову пошту, а також миттєві та текстові повідомлення (SMS). Фактично, це масове розсилання кореспонденції рекламного чи іншого характеру абонентам, які не висловили бажання її одержувати [8].
Фішингові повідомлення	це електронні листи, надіслані через Інтернет-мережу, SMS або інші повідомлення, що схожі на запити від офіційних організацій (установ) і здатні розкривати (викрадати) персональні дані користувачів. Фішинг можливий через шахрайське повідомлення електронної пошти або спеціально створений сайт. Зазвичай, фішинг у мережі Інтернет починається з отримання користувачем повідомлення електронною поштою, яке імітує електронного листа, що надійшов з надійного джерела, відомого користувачеві. В електронному листі міститься посилання на підроблений веб-вузол або сайт, де потрібно ввести особисту інформацію,

Назва шкідливого програмного продукту	Коротка характеристика
	наприклад, логіни, паролі, коди активації, особисту або фінансову інформацію. Запобігти фішингу можна шляхом уважного ставлення до адрес сайтів, на які відбувається перехід за посиланням [29; 20].
DDoS-атаки (розподілені атаки на відмову в обслуговуванні)	це випадки DoS (Denial of Service, відмова в обслуговуванні), коли вебсайт жертви (мережа чи інший онлайн-сервіс) атакується не з одного джерела, а одночасно з багатьох напрямків, з метою перевантажити великою кількістю підроблених або небажаних запитів. Фактично, це мережева кібератака, за допомогою якої, наприклад, намагаються переобтяжити сайт, вичерпати його ресурси і досягти стану, щоб він почав гальмувати, не міг відповідати на нові запити клієнтів, став недоступний для звичайних користувачів одержувати [8; 16].
Шпигунські програми (програми-шпигуни)	це різновид шкідливого програмного забезпечення, завданням якого є збір інформації про користувача і прихована передача цієї інформації на сайт розробника. Зазвичай, шпигунські програми, на відміну від троянських програм, не викрадають і не передають паролі, номери кредитних карт та іншу конфіденційну інформацію. Проте, вони можуть передавати дані про конфігурацію комп'ютера, встановлене програмне забезпечення, дії користувача і т.п. Нерідко шпигунські програми являють собою панелі, що розширюють можливості браузера (вебпереглядача, вебоглядача, вебнавігатора). Подібне є надзвичайно зручним для таємного спостереження за роботою користувача у мережі Інтернет. Крім того, шпигунські програми можуть виводити на екран рекламу (наприклад, спливаючі оголошення), збирати відомості про користувача, змінювати параметри комп'ютера або втручатися в роботу браузера без згоди користувача. На основі програм-шпигунів створюються програми-вимагачі, які показують спливаючі оголошення [29].
Програми-вимагачі (Ransomware)	це різновид шкідливого програмного забезпечення, яке може бути представлене кількома різними способами та негативно впливати на окремі електронні системи і мережі юридичних та/або фізичних осіб, а саме: фішинг-листи – це періодична форма розповсюдження шкідливих програм коли жертви заражаються через компрометовані вкладення електронної пошти або посилання, замасковані під законні; Exploit Kits – це пакет, виготовлений з різних шкідливих інструментів і попередньо написаного коду експлуатації з метою використання проблем та вразливостей програмних додатків й операційних систем як способу розповсюдження шкідливого програмного забезпечення (найпоширенішими цілями є небезпечні системи, що працюють із застарілим програмним забезпеченням); зловживання рекламою, коли зловмисники використовують рекламні мережі для розповсюдження програм-вимагачів. По суті, це зловмисне програмне забезпечення, що блокує електронний пристрій або шифрує його вміст, з метою відновлення доступу до інфікованого комп’ютера та/або даних за певну плату [8; 19].

Назва шкідливого програмного продукту	Коротка характеристика
Перехоплювач паролів	це різновид шкідливого програмного забезпечення для крадіжки паролів та облікових даних у процесі обігу користувачів до терміналів аутентифікації інформаційної системи. Така програма здійснює спроби заволодіти обліковими даними, що дозволяють, не викликаючи жодних підозр, абсолютно санкціоновано проникнути до інформаційної системи, оминаючи службу інформаційної безпеки, яка нічого не запідозрює. Зазвичай, перехоплювач паролів ініціює помилку під час аутентифікації і користувач, вважаючи, що помилився при введенні пароля, повторно вводить облікові дані для входу до системи. Таким чином, як правило, ці дані стають відомі власнику перехоплювача паролів, тому, подальше використання старих облікових даних є небезпечним [29].

Джерело: розроблено авторами за результатами дослідження.

Як можна пересвідчитися, шкідливі програмні продукти (шкідливий програмний засіб, шкідливе програмне забезпечення (англ. malware – скорочено від malicious – зловмисний і software – програмне забезпечення)) – це спеціальні програми або мобільні коди, які, отримавши доступ до державних (службових, приватних) інформаційних систем, перешкоджають технологічно-паспортному функціонуванню комп'ютера (сервера) і зменшують продуктивність його роботи, пошкоджують бази даних та/або інфокомунікаційну мережу (digital-канали), викрадають конфіденційну інформацію, що заважає нормальній діяльності фізичних та/або юридичних осіб, несе загрозу державній (службовій, приватній) таємниці (сформовано авторами за результатами дослідження). Наприклад, шкідливі програмні продукти максимально негативно вливають на діяльність органів державної влади та військового управління, що призводить до відмови, як правило, електронних систем, які інтегровані в загально-організаційні системи управління і технологічні процеси надання послуги, а також – до знищення офіційних даних, розміщених на електронних носіях інформації. З огляду на це варто зазначити, що у цілому, до електронної системи входить будь-який електронний блок, вузол, прилад або комплекс таких приладів, як сукупність електронних компонентів, що здійснює обробку інформації, а електронними

носіями інформації, зазвичай, є матеріальні електронні носії (жорсткі диски, флеш-пам'ять, CD, DVD, Blue-ray, диски дискети, касети на магнітній стрічці і т. ін), що використовують для реєстрації (записування), зберігання і відтворення інформації (даних), обробленої засобами комп'ютерної (обчислювальної) техніки.

Натомість, не зважаючи на означені ризики, основними перешкодами у процесі забезпечення захисту від кіберзагроз є бюджетні обмеження, а головне, не усвідомлення адміністрацією (апаратом управління) того, що дієвість впливу будь-якої базової системи адміністративного менеджменту та, як наслідок, ефективність загально-організаційної системи управління і продуктивність роботи кожного структурного підрозділу і штатного працівника, стійкі конкурентні й репутаційні переваги органів державної влади та військового управління, прямо залежать від тотальності цифрової трансформації та безперебійної роботи всіх технологічно важливих процесів, процедур і процесів організування роботи. Враховуючи вищезазначене, в Україні дигіталізація стає обов’язковою до впровадження, адже цифрові технології охоплюють всі сфери розбудови держави і життя громадян, а національні підходи до кібербезпеки гарантують її дієвість на загальнонаціональному і місцевому рівні. Для цього прийнято нормативні документи:

− Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року “Про Стратегію кібербезпеки України”» від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 05.12.2022).

− Закон України «Про інформацію» від 02 жовтня 1992 року № 2657-XII;

− Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 05 липня 1994 року № 80/94-ВР;

− Закон України «Про Концепцію Національної програми інформатизації» від 04 лютого 1998 року № 75/98-ВР;

− Закон України «Про електронні документи та електронний документообіг» від 22 травня 2003 року № 851-IV;

− Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 09 січня 2007 року № 537-V;

− Закон України «Про захист персональних даних» від 01 червня 2010 року № 2297-VI;

− Закон України «Про доступ до публічної інформації» від 13 січня 2011 року № 2939-VI;

− Закон України «Про адміністративні послуги» від 06 вересня 2012 року № 5203-VI;

− Закон України «Про основні засади забезпечення кібербезпеки України» від 05 жовтня 2017 року № 2163-VIII;

− Закон України «Про електронні довірчі послуги» від 05 жовтня 2017 року № 2155-VIII;

− Закону України «Про особливості надання публічних (електронних публічних) послуг» від 15 липня 2021 року № 1689-IX;

− Закон України «Про Національну програму інформатизації» від 01 грудня 2022 року № 2807-IX;

− ДСТУ ISO/IEC 33001:2016 «Інформаційні технології. Оцінювання процесу. Поняття та термінологія» (ISO/IEC 33001:2015, IDT). Наказ ДП «УкрНДНЦ» від 27.12.2016 року № 447.

Отже, як свідчить загально світовий досвід та аналіз надання електронних публічних послуг державними інституціями й органами військового управління у розвинених країнах, рівень дієвості використання базової системи адміністративного менеджменту – основи конкурентних і репутаційних переваг в умовах глобалізації, безпосередньо пов’язана з рівнем тотального застосування продуктивних цифрових технологій та пропускної спроможності інфокомунікаційних мереж, що мають гарантувати належне якісно-оперативне організування і забезпечення процесів адміністрування управління та продуктивну взаємодію із заінтересованими сторонами. Це пояснюється тим, що, фактично, дигіталізація виконує такі завдання [4]:

− якісно змінює внутрішньо-організаційну інформаційну політику;

− спонукає використовувати на практиці новий механізм вироблення, прийняття і реалізації адміністративних рішень (оперативних, поточних, стратегічних);

− стимулює регулярно підвищувати фаховість кожного штатного працівника, задіяного у наданні послуг, і ділову досконалість органів державної влади та військового управління загалом;

− гарантує створення привабливо-високооплачуваних і високотехнологічних робочих місць;

− вимагає регулярної модернізації цифрових технологій і засобів їх реалізації (можливо, навіть, завдяки власним напрацюванням);

− оптимізує інформаційні потоки і комунікаційні ланцюги із заінтересованими сторонами;

− забезпечує інформаційну підтримку діяльності окремих штатних працівників, структурних підрозділів, органів державної влади та військового управління загалом на основі сучасних цифрових технологій та інтелектуальних систем;

− сприяє адаптованості, продуктивності, своєчасності й результативності виконання посадових обов’язків і виробничих завдань;

− підвищує якість, безпечність та конкурентоздатність послуг;

− нарощує конкурентні й репутаційні переваги органів державної влади та військового управління;

− привертає увагу потенційних інвесторів для яких цифрові трансформації є головним показником якісного рівня ділової досконалості;

− позитивно впливає на збільшення числа і різноманіття наданих послуг та отриманих позитивних результатів роботи.

Висновки та перспективи подальших розвідок у даному напрямі. Фахове усвідомлення адміністрацією (апаратом управління) доцільності використання переваг тотально-оптимальної й адаптовано-раціональної дигіталізації з метою гарантування дієвості розвитку та ефективності використання базової системи адміністративного менеджменту органів

державної влади та військового управління за умови глобалізації світу беззаперечно та об’єктивно стає головною умовою переходу на якісно новий рівень цифровізації, що, по суті, слугує також основою для кожного з етапів запровадження й удосконалення управлінських новацій, у тому числі, однієї з моделей ділової досконалості. У будь-якому випадку, практична потреба інструментарію дигіталізації, з метою унормування обов’язковості його застосування, має бути відображена у кожному внутрішньо-організаційному (адміністративному) документі, що окреслює місце і роль окремо взятого елемента й підсистеми базової системи адміністративного менеджменту. Водночас, з метою набуття юридично-адміністративної ваги, покрокові дії щодо тотальної дигіталізації мають бути визначені Положенням «Про інформаційну політику юридичної особи». Норми цього Положення зобов’язані свідомо, відповідально і фахово сприйматися й виконуватися всіма заінтересованими сторонами конкретної юридичної особи, особливо штатними працівниками, як сукупність основних напрямів і способів діяльності зі створення розвиненого інформаційного середовища, модернізації інформаційної інфраструктури, розвитку інформаційних і телекомунікаційних технологій заради підвищення продуктивності та гарантування своєчасно-результативної роботи, ефективного формування (одержання), зберігання і використання інформаційних ресурсів шляхом забезпечення вільного доступу до них (за винятком конфіденційних), а також, за потреби, – з інформування конкретного споживача або поширення суспільно вагомої інформації на загал. Вагоме значення акцентованого спонукатиме проводити подальші розвідки у цьому напрямі, враховуючи специфіку роботи органів державної влади та військового управління, а також можливу поведінку факторів їх внутрішнього і зовнішнього середовища прямої та непрямої дії.

Література

1. Андрощук Г. Індекс цифрової економіки і суспільства 2020 (DESI 2020). Юридична газета online. 06.08.2020. URL: https://yur-gazeta.com/golovna/indeks-cifrovoyi-ekonomiki-i-suspilstva-2020-desi-2020.html (дата звернення: 15.06.2023).

2. Андрощук Г. О. Цифрова транформація європейської економіки: стан та місце України. *Інформація і право.* 2023. № 1 (44). С. 67–78.

3. Віруси, трояни та хробаки: що це таке і як вберегти свою техніку? 2020. URL: https://indevlab.com/uk/blog-ua/virusi-troyani-ta-hrobaki-shho-tse-take-i-yak-vberegti-svoyu-tehniku (дата звернення: 15.06.2023).

4. Гудзь О.Є., Федюнін С. А., Щербина В. В. Диджиталізація, як конкурентна перевага підприємств. *Економіка. Менеджмент. Бізнес.* 2019. № 3 (29). DOI: 10.31673/2415-8089.2019.031824

5. Даниленко Ю. Від Ш до І: що таке штучний інтелект та як він трансформує світ. 2022. URL: https://speka.media/ai/vid-s-do-i-shho-take-stucnii-intelekt-ta-yak-vin-transformuje-svit-xv7039 (дата звернення: 15.06.2023).

6. Детально про віртуалізацію: типи, переваги та рішення. 2021. URL: https://onbiz.biz/about-virtualization (дата звернення: 15.06.2023).

7. Дистанційна ідентифікація. Термінологічний словник з питань запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму, фінансуванню розповсюдження зброї масового знищення та корупції / редак. колег. А. Г. Чубенко, М. В. Лошицький, Д. М. Павлов, С. С. Бичкова, О. С. Юнін. Київ: Ваіте, 2018. С. 216.

8. Комп’ютерний вірус. 2023. URL: https://www.eset.com/ua/support/information/ entsiklopediya-ugroz/kompyuternyy-virus/ (дата звернення: 15.06.2023).

9. Комп’ютерний хробак. (2022). URL: https://uk.wikipedia.org/wiki/Комп%27ютерний_хробак (дата звернення: 15.06.2023).

10. Міненко М. А., Піддубний В. А. Організація, організування, адміністрування. *Економіка АПК*. 2021. № 12. С. 33–45.

11. Побудова систем віртуалізації. 2023. URL: https://techexpert.ua/it-services/building-of-virtualization-systems/ (дата звернення: 15.06.2023).

12. Про Національну програму інформатизації : Закон України від 01.12.2022 № 2807-IX. URL: https://zakon.rada.gov.ua/laws/show/2807-20#Text (дата звернення: 15.06.2023).

13. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 15.06.2023).

14. Халапсис А. В. Глобализация и метрика истории. *Економіка. Менеджмент. Бізнес*. 2019. № 3 (29). URL: http://halapsis.net/globalizatsiya-i-metrika-istorii (дата звернення: 15.06.2023).

15. Чернишев Д. О., Рижаков Д. А., Хоменко О. М., Петруха С. В., Кучеренко О. І., Горбач М. В. Цифрові технології як інноваційні тренди структурно-трансформаційних зрушень у системі управління підприємств-стейкхолдерів будівництва. *Управління розвитком складних систем*. 2021. №46. С. 118–130. DOI : https://doi.org/10.32347/2412-9933.2021.46.118-130.

16. Що таке *DDoS* атаки та яку мету вони переслідують. 2022. URL: https://infocom.ua/що-таке-ddos-атаки/ (дата звернення: 15.06.2023).

17. Що таке блокчейн? 2021. URL: https://egera.com/uk/shcho-take-blokcheyn (дата звернення: 15.06.2023).

18. Що таке доповнена реальність? 2023. URL: https://teach-hub.com/scho-take-dopovnena-realnist (дата звернення: 15.06.2023).

19. Що таке програми-вимагачі (Ransomware)? 2021. URL: https://cryptoacademy.com.ua/shho-take-programy-vymagachi-ransomware (дата звернення: 15.06.2023).

20. Що таке фішинг і фішингова атака. 2022. URL: https://hostiq.ua/blog/ukr/internet-phishing (дата звернення: 15.06.2023).

21. Що таке хмарні технології і навіщо вони потрібні. 2022. URL: https://edin.ua/shho-take-xmarni-texnologi%D1%97-i-navishho-voni-potribni (дата звернення: 15.06.2023).

22. De Clerck, J.-P. Digitization, digitalization, and digital transformation: the differences. 2020. URL: https://www.i-scoop.eu/digitization-digitalization-digital-transformation-disruption (accessed : 15 June 2023).

23. Grünenberg, K., Mohl, P., Fog, K. O. & Simonsen, A. Issue Introduction: IDentities and Identity: Biometric Technologies, Borders and Migration. *Ethnos,* 2022. Vol. 87. № 2. P. 211–222. DOI: 10.1080/00141844.2020.1743336.

24. Kuvnako A., Mahamatov N., Kuznetsova V., Mukhtarova G., Malikova N., Atadjanova M. A Practical Approach To The Development Of A Decision-Supporting System Based On Fuzzy Neural Network In Information And Telecommunication Systems. *IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS),* Toronto ; ON, Canada, 2022. P. 1–4. DOI: 10.1109/IEMTRONICS55184.2022.9795724.

25. Lexico powered by Oxford. 2023. URL: https://en.oxforddictionaries.com/definition/digital (accessed : 15 June 2023).

26. Mahmood A., Akram T, Chen H. F, Chen S. G. On the Evolution of Additive Manufacturing (3D/4D Printing) Technologies: Materials, Applications, and Challenges. *Polymers,* 2022. Vol. 14. № 21. DOI: 10.3390/polym14214698.

27. Munteanu P., Ciornei L. The impact of business digitization on the three pillars of sustainable development. *Proceedings of the International Conference on Business Excellence*. 2020. Vol. 14. № 1. P. 343–351. DOI: 10.2478/picbe-2020-0033.

28. Oxford English Dictionary (2nd ed.) / J. Simpson & E. Weiner (Eds.). Clarendon Press. Revised. 2010. URL: https://www.oed.com/viewdictionaryentry/Entry/52611 (дата звернення: 15.06.2023).

29. Rebenok V., Al-Namri R., Butko O., Fedorenko V., Tereshchenko O., Tsimokh N. Infocommunication Technologies In Education: Problems Of Implementation. *IJCSNS International Journal of Computer Science and Network Security,* December 2021. Vol. 21. № 12. P. 41–44. URL: http://paper.ijcsns.org/07_book/202112/20211206.pdf (дата звернення: 15.06.2023).

30. Ritter T. Digitization capability and the digitalization of business models in business-to-business firms: Past, present, and future. *Industrial Marketing Management,* 2020. Vol. 86. P. 180–190. DOI: 10.1016/j.indmarman.2019.11.019.

References

1. Androshchuk, G. (2020), "Digital Economy and Society Index 2020"*, Legal Newspaper Online*, [Online], available at: https://yur-gazeta.com/golovna/indeks-cifrovoyi-ekonomiki-i-suspilstva-2020-desi-2020.html (Accessed 15 June 2023).

2. Androshchuk, G. O. (2023), "Digital transformation of the European economy: the state and place of Ukraine.", *Information and Law*, vol. 1(44), pp. 67-78.

3. Indevlab (2020), "Viruses, Trojans, and worms: What are they and how to protect your devices?", available at: https://indevlab.com/uk/blog-ua/virusi-troyani-ta-hrobaki-shho-tse-take-i-yak-vberegti-svoyu-tehniku (Accessed 15 June 2023).

4. Houdz, O. Ye., Fedyunin, S. A., & Shcherbina, V. V. (2019), "Digitalization as a competitive advantage of enterprises", *Economics. Management. Business*,vol. 3(29). doi: 10.31673/2415-8089.2019.031824.

5. Danilenko, Y. (2022), "From A to I: What is artificial intelligence and how does it transform the world", available at: https://speka.media/ai/vid-s-do-i-shho-take-stucnii-intelekt-ta-yak-vin-transformuje-svit-xv7039 (Accessed 15 June 2023).

6. TechExpert (2021), "In-depth about virtualization: Types, advantages, and solutions", available at: https://onbiz.biz/about-virtualization (Accessed 15 June 2023).

7. Chubenko, A. G., Loshitskiy, M. V., Pavlov, D. M., Bychkova, S. S., & Yunin, O. S. (2018), "Remote identification", Terminolohichnyj slovnyk z pytan'

zapobihannia ta protydii lehalizatsii (vidmyvanniu) dokhodiv, oderzhanykh zlochynnym shliakhom, finansuvanniu teroryzmu, finansuvanniu rozpovsiudzhennia zbroi masovoho znyschennia ta koruptsii [Terminological dictionary on preventing and countering money laundering, financing terrorism, financing the proliferation of weapons of mass destruction, and corruption], Vaite, Kyiv, Ukraine.

8. Eset (2023), "Computer virus", available at: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/kompyuternyy-virus (Accessed 15 June 2023).

9. Wikipedia (2022), "Computer worm" available at: https://uk.wikipedia.org/wiki/Комп%27ютерний_хробак (Accessed 15 June 2023).

10. Minenko, M. A., & Piddubnyi, V. A. (2021), "Organization, organizing, administration", *Economics of Agro-Industrial Complex*, vol. 12, pp. 33-45.

11. TechExpert (2023), "Building virtualization systems", available at: https://techexpert.ua/it-services/building-of-virtualization-systems (Accessed 15 June 2023).

12. The Verkhovna Rada of Ukraine (2022), The Law of Ukraine "On the National Program of Informatization", available at: https://zakon.rada.gov.ua/laws/show/2807-20#Text (Accessed 15 June 2023).

13. The Verkhovna Rada of Ukraine (2017), The Law of Ukraine "On the Fundamental Principles of Cybersecurity of Ukraine", available at: https://zakon.rada.gov.ua/laws/show/2163-19#Text (Accessed 15 June 2023).

14. Khalapsis, A. V. (2019), "Globalization and the metrics of history", *Economics. Management. Business*, vol. 3, available at: http://halapsis.net/globalizatsiya-i-metrika-istorii (Accessed 15 June 2023).

15. Chernyshev, D. O., Ryzhakov, D. A., Khomenko, O. M., Petrucha, S. V., Kucherenko, O. I., & Gorbach, M. V. (2021), "Digital technologies as innovative trends of structural-transformative changes in the management system of construction stakeholder enterprises", *Management of Complex Systems Development*, vol. 46, pp. 118-130, doi: 10.32347/2412-9933.2021.46.118-130.

16. Infocom (2022), “What are DDoS attacks and their objectives”, available at: https://infocom.ua/що-таке-ddos-атаки/ (Accessed 15 June 2023).

17. Egera (2021), “What is blockchain?”, available at: https://egera.com/uk/shcho-take-blokcheyn (Accessed 15 June 2023).

18. Teach-hub (2023), “What is augmented reality?”, available at: https://teach-hub.com/scho-take-dopovnena-realnist (Accessed 15 June 2023).

19. Cryptoacademy (2021), “What are ransomware programs?”, available at: https://cryptoacademy.com.ua/shho-take-programy-vymagachi-ransomware (Accessed 15 June 2023).

20. Hostiq (2022), “What is phishing and phishing attack”, available at: https://hostiq.ua/blog/ukr/internet-phishing (Accessed 15 June 2023).

21. Edin (2022), “What are cloud technologies and why are they needed”, available at: https://edin.ua/shho-take-xmarni-texnologi%D1%97-i-navishho-voni-potribni (Accessed 15 June 2023).

22. De Clerck, J.-P. (2020), “Digitization, digitalization, and digital transformation: The differences”, available at: https://www.i-scoop.eu/digitization-digitalization-digital-transformation-disruption (Accessed 15 June 2023).

23. Grünenberg, K., Mohl, P., Fog, K. O. & Simonsen, A. (2022), “Issue Introduction: IDentities and Identity: Biometric Technologies, Borders and Migration”, *Ethnos,* vol. 87:2, pp. 211-222, doi: 10.1080/00141844.2020.1743336.

24. Kuvnako, A., Mahamatov, N., Kuznetsova, V., Mukhtarova, G., Malikova, N. and Atadjanova, M. (2022), “A Practical Approach To The Development Of A Decision-Supporting System Based On Fuzzy Neural Network In Information And Telecommunication Systems”, *IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS),* Toronto, ON, Canada, pp. 1-4, doi: 10.1109/IEMTRONICS55184.2022.9795724.

25. Lexico powered by Oxford (2023), available at: https://en.oxforddictionaries.com/definition/digital (Accessed 15 June 2023).

26. Mahmood, A ., Akram, T, Chen, H.F, Chen, S.G. (2022), “On the Evolution of Additive Manufacturing (3D/4D Printing) Technologies: Materials,

Applications, and Challenges", *Polymers,* vol. 14(21), p. 4698, doi: 10.3390/polym14214698.

27. Munteanu, P. and Ciornei, L. (2020), "The impact of business digitization on the three pillars of sustainable development", *Proceedings of the International Conference on Business Excellence*, vol. 14, is. 1, pp. 343-351. doi: 10.2478/picbe-2020-0033.

28. Simpson, J. & Weiner, E. (2010), Oxford English Dictionary, 2nd ed., Clarendon Press, Oxford, UK, available at: https://www.oed.com/viewdictionaryentry/Entry/52611 (Accessed 15 June 2023).

29. Rebenok, V., Al-Namri, R., Butko, O., Fedorenko, V., Tereshchenk, O., Tsimokh, N. (2021), "Infocommunication Technologies In Education: Problems Of Implementation", *IJCSNS International Journal of Computer Science and Network Security,* vol. 21, is. 12, pp. 41-44. Retrieved from http://paper.ijcsns.org/07_book/202112/20211206.pdf (Accessed 15 June 2023).

30. Ritter, T. (2020), "Digitization capability and the digitalization of business models in business-to-business firms: Past, present, and future", *Industrial Marketing Management,* vol. 86, pp. 180-190, doi: 10.1016/j.indmarman.2019.11.019.

Стаття надійшла до редакції 12.09.2023 р.