ДИДЖИТАЛІЗАЦІЯ: ЗАГАЛЬНІ ПРОБЛЕМИ ТА ПИТАННЯ КІБЕРБЕЗПЕКИ

DIGITALIZATION: GENERAL PROBLEMS AND CYBERSECURITY ISSUES

УДК 339.65.011:342.9
DOI: https://doi.org/10.32843/infrastruct81-11

Сергієнко О.А.[1]
д.е.н., професор,
професор кафедри підприємництва,
торгівлі і логістики,
Національний технічний університет
«Харківський політехнічний інститут»
Іпполітова І.Я.[2]
к.е.н., доцент,
доцент кафедри підприємництва,
торгівлі і логістики,
Національний технічний університет0
«Харківський політехнічний інститут»
Савченко Р.О.[3]
аспірант кафедри підприємництва,
торгівлі і логістики,
Національний технічний університет
«Харківський політехнічний інститут»

Serhiienko Olena
National Technical University
"Kharkiv Polytechnic Institute"
Ippolitova Inna
National Technical University
"Kharkiv Polytechnic Institute"
Savchenko Roman
National Technical University
"Kharkiv Polytechnic Institute"

В статті визначено, що диджиталізація стає одним із головних факторів інноваційного розвитку будь-якої країни. Зосереджено увагу на позитивних наслідках цього процесу та його впливу на соціально-економічний розвиток країни, галузей економіки та окремих бізнесів. Було визначено переваги та можливості, які надає процес цифровізації. Виокремлено проблеми, пов'язані з диджиталізацією та зосереджено увагу на питаннях кібербезпеки. Наведено приклади найвідоміших кібератак, що мали місце у першій чверті XXI сторіччя та зазначено причини, які призвели їх до успіху. Визначено перелік ризиків, пов'язаних із проведенням цифровізації. Описано, що нехтування питаннями кібербезпеки та кіберзагроз великою мірою уповільнює процес цифрової трансформації. Наголошено, що для успішної диджиталізації бізнес-процесів необхідно, розробити та впровадити відповідні державні політики, забезпечити достатній рівень інвестування в захисну інфраструктуру, а також розробити та впровадити сприятливу законодавчу базу.
Ключові слова: *диджиталізація, цифрові технології, кібербезпека, кіберзагроза, кібератака.*

The article has established that digitalization is becoming one of the key drivers of innovative development in modern economies. It emphasizes the positive impacts of this process on the socio-economic growth of nations, economic sectors, and individual businesses. The adoption of digital technologies enables process automation, boosts operational efficiency, improves the quality of services, and unlocks new opportunities for innovation. The article outlines the advantages and potential offered by digitalization while also addressing the challenges it brings, particularly in the area of cybersecurity. Specific examples of the most significant cyberattacks of the 21st century are examined, highlighting the factors that contributed to their success. A comprehensive list of risks associated with digitalization is identified, including dependence on technology, ethical dilemmas, social and economic implications, legal and regulatory issues, cultural transformations, impacts on mental health, and threats to cybersecurity. These risks underline the complexity of the digital transformation process and the importance of addressing them to ensure sustainable development. The article stresses that successful digitalization of business processes requires the implementation of robust government policies, sufficient investment in protective infrastructure, continuous personnel training, awareness-raising programs, and the creation of a favorable legislative environment. Such measures not only protect critical information resources and infrastructure but also build trust among citizens and businesses in digital technologies. The article's practical significance lies in the proposed comprehensive system of measures aimed at strengthening cybersecurity. These measures include developing specialized legislation, investing in security infrastructure, and fostering a culture of digital literacy. Systematic implementation of these initiatives will lead to the creation of a reliable cybersecurity framework that not only safeguards digital transformation but also stimulates its development at both the enterprise and national levels.
Keywords: *digitalization, digital technologies, cybersecurity, cyberthreats, cyberattack.*

Постановка проблеми. Сьогодні диджиталізація перетворюється на ключовий фактор розвитку суспільства та економіки. Вона кардинально змінює спосіб, у який відбувається повсякденне спілкування, робочі процеси, навчання та взаємодія з навколишнім світом. Цифрові технології стають основою функціонування багатьох галузей, починаючи від фінансових і банківських послуг до охорони здоров'я, транспорту, освіти та державного управління. Розвиток диджиталізації створює нові можливості для інновацій та підвищення ефективності в різних сферах життя. Однак, разом із прогресом приходять і нові виклики. Серед них – адаптація до швидкозмінних технологій, забезпечення рівного доступу до цифрових ресурсів та збереження етичних стандартів у диджиталізованому світі. Одним із найактуальніших питань у цьому контексті є кібербезпека. Зі збільшенням обсягів даних, які зберігаються та передаються в електронному вигляді, виникають загрози витоку інформації, хакерських атак, фішингу, а також інших форм кіберзлочинності.

Аналіз останніх досліджень і публікацій. Питанням диджиталізації (цифровізації) у сучасній Україні приділяється досить велика увага. Вітчизняні фахівці зосереджують увагу на питаннях використання цифрових технологій у першу чергу з метою прокращення процесів ведення бізнесу, підвищення доходу від провадження підприємницької діяльності та удосконалення системи комунікації з партнерами та споживачами.

Так Лапін А.В., Грінчук І.О. та Оленюк Д.О. [1] досліджують підходи до визначення терміну «диджиталізація» та виводять власне формулювання цього поняття, приділяють увагу її складовим частинам, окреслюють притаманні переваги та недоліки, аналізують особливості, що їх має процес цифровізації в різних галузях економіки,

[1] ORCID: https://orcid.org/0000-0002-9796-9218
[2] ORCID: https://orcid.org/0000-0003-3981-3992
[3] ORCID: https://orcid.org/0009-0006-6903-9925

роблять висновки щодо позитивного впливу диджиталізації на підприємництво та наголошують, що найбільшої ефективності для держави можна досягти за можливості використання досягнень цифровізації у всіх сферах суспільного життя.

Шлайфер М.Б., Тодощук А.В. [2] досліджують питання диджиталізації економіки країни через призму процесів євроінтеграції. Вони розглядають її як первний стимул для інноваційного розвитку, що не тільки відкриває нові можливості (гнучкість і персоналізація продукції), але й створює нові виклики (швидкі технологічні зміни та високі вимоги законодавства). Науковці підкреслюють, що інтеграція України у глобальні цифрові процеси сповільнюються слабкою диджиталізацією державного управління, недостатнім доступом до технологій та інвестиційними ризиками.

Саврас І.З., Фединець Н.І. [3] присвячують власні дослідження інноваційній діяльності підприємств в умовах цифровізації, зосереджуючи увагу на проблемах і перспективах впровадження інновацій, взаємозв'язку між цифровими технологіями та інноваційною діяльністю. Також вони наголошують, що цифровізація сприяє прискоренню управлінських рішень та адаптації до ринкових змін, створюючи нові конкурентні можливості, рекомендують подальший аналіз впровадження цифрових технологій вітчизняними підприємствами.

Водянка Л.Д. та Стахова Н.П. [4] розглядають цифровізацію як «трансформацію бізнесу через цифрові технології для оптимізації процесів і взаємодії з клієнтами, співробітниками та постачальниками». На їх погляд, вона охоплює економіку віртуальних світів, штучний інтелект, роботизацію, електронні гроші та великі дані, наголошують, що в нашій країні вона зосереджена на підвищенні продуктивності та нових способах отримання доходу, підкреслюють, що ключовим фактором розвитку є інновації, зокрема в клієнтському досвіді, операційних процесах та бізнес-моделях.

Данилишин В.І. та Синиця С.М. [5] зосереджують свою увагу на диджиталізації фінансових послуг – переході від традиційних сервісів до використання сучасних технологій, що підвищує ефективність управління фінансами та покращує доступність і якість послуг. В Україні цей процес стає ключовим фактором трансформації фінансового сектора, сприяючи розвитку електронних платежів, мобільного банкінгу, електронних кредитів, фінтех-рішень і кібербезпеки. Основні переваги включають зручність для клієнтів, зниження витрат і розширення ринку.

Небога Т.В. та Лабунська О.Б. [6] досліджують процес диджиталізації бізнес-суб'єктів в Україні з використанням інформаційно-комунікаційних технологій, а також аналізують їх доступ до Інтернету залежно від видів економічної діяльності. Вони вказують, що для успішної диджиталізації необхідна ефективна інноваційна інфраструктура, а управління бізнесом в цифрову епоху вимагає створення цифрової екосистеми, включаючи швидкісну мережу Інтернет.

Як можна побачити з наведеного вище, вітчизняні фахівці зосереджують свою увагу на позитивному впливі, що процеси диджиталізації здійснюють на економічний розвиток України загалом та окремих її галузей чи певних підприємств зокрема. У той самий час питання проблем, що їх породжує цифровізація, залишаються поза їх увагою та розглядаються спеціалістами з окремих питань. У той час як недостатня увага до проблем, що пов'язані із розвитком диджиталізації, та їх вирішення може гальмувати сам проце цифровізації та звести нанівець усі здобутки від його впровадження.

Постановка завдання. Метою дослідження є узагальнення основних проблем, які виникають під час запровадження підприємствами диджиталізації й забезпечення кібербезпеки та формування комплексної системи заходів, спрямованих на мінімізацію ризиків, пов'язаних з кіберзагрозами.

Виклад основного матеріалу дослідження. В загальному розумінні, диджиталізація (або цифровізація) – це процес впровадження цифрових технологій у різні аспекти життя та бізнесу [7]. Він включає перехід від аналогових до цифрових систем, що дозволяє автоматизувати процеси, покращувати обмін даними і підвищувати ефективність різних видів діяльності. Однією з таких проблем, є питання кібербезпеки – що можна розглядати як одну з ключових проблем у провадженні диджиталізації в Україні. Зі зростанням впровадження цифрових технологій та послуг, зростає і кількість кіберзагроз, які можуть негативно вплинути на безпеку даних, конфіденційність інформації та цілісність бізнес-процесів. Відсутність достатньої уваги до кібербезпеки є серйозною перешкодою для ефективної диджиталізації. Підвищення рівня усвідомленості щодо загроз, інвестування в інфраструктуру захисту, навчання персоналу та розробка чіткої нормативної бази є важливими кроками для забезпечення безпеки в цифровому середовищі. Це дозволить не лише знизити ризики, але й підвищити загальну ефективність бізнес-процесів у країні.

У сучасному світі, диджиталізація стає потужним двигуном прогресу суспільства, надаючи численні можливості для підвищення ефективності та зручності в різних сферах життя. Сьогодні технології відіграють важливу роль у бізнесі, освіті, охороні здоров'я та державному управлінні. Завдяки діжиталізації підприємства здатні автоматизувати рутинні процеси, що дозволяє знижувати витрати і підвищувати продуктивність. Клієнти можуть отримувати швидкі послуги, а бізнес має можливість швидше реагувати на зміну попиту. У сфері освіти диджиталізація відкриває доступ до онлайн-курсів,

вебінарів та інших ресурсів, що дозволяє кожному навчатися у зручному для нього темпі та в будь-який час. Окрім того, в умовах диджиталізації громадяни мають можливість отримувати державні послуги через онлайн-платформи, що знижує бюрократію та покращує доступ до інформації. У сфері охорони здоров'я технології забезпечують покращений доступ до медичних послуг, дозволяючи пацієнтам отримувати консультації дистанційно та слідкувати за своїм здоров'ям за допомогою мобільних додатків. Усі ці позитивні наслідки цифровізації можна поділити на декілька груп, що відбражають основні ознаки (аспекти) цього процесу. Приклад такого розподілу можна побачити на рисунку 1.

Зазначені ознаки притаманні й Україні, в якій диджиталізація виступає одним із ключових напрямів розвитку на національному рівні. Про це свідчать такі характеристики:

1. Широке розповсюдження користування національним порталом та мобільним додатком Дія, що надає громадянам доступ до низки державних послуг, таких як реєстрація бізнесу, отримання документів та багато іншого. Дія також включає систему електронних паспортів.

2. Використання в процесі здійснення купівель, сплати послуг, здійснення фінансових операцій мережі Інтернет та онлайн-майданчики.

3. Активний розвиток онлайн-освітніх платформи (Prometheus та EdEra), які надають безкоштовні курси з різних тем.

4. Розвиток цифрової інфраструктури, включаючи широкосмуговий інтернет у сільських та віддалених регіонах, є пріоритетом для уряду України.

Тому диджиталізація в Україні сприяє підвищенню прозорості, покращенню доступу до державних послуг та спрощенню взаємодії між державою та громадянами. Крім того, диджиталізація надає переваги для пересічних громадян, підприємців та держави загалом. Проте, процеси цифровізації також пов'язані з низкою потенційних небезпек та ризиків, серед яких: залежність від технологій, етичні питання, соціальні та економічні наслідки, правові та регуляторні проблеми, культурні зміни, вплив на психічне здоров'я та кібербезпека. Розглянемо більш детально кожну з потенційних загроз.

Що стосується залежності від технологій, то вона буде проявлятися в тому, що будь-який технічний збій або збій у роботі технічних систем може призвести до значних втрат і збоїв у роботі підприємства. Також така залежність може привести до втрати навичок, що зробить їх залежними від інформаційних технологій. На сьогодні така залежність не вбачається чимось занадто небезпечним, але, враховуючи швидкість розвитку цифрових технологій у новітньому світі, ситуація може змінитися вже за кілька років. Диджиталізація – це також процес, який може вплинути на етичні питання. Перше за все ті, що з'являються із розвитком штучного інтелекту та пов'язані з процесом прийняття рішень без участі людини. По-друге – збір та використання біометричних даних, що вже

Рис. 1. Основні аспекти диджиталізації (цифровізації)

Джерело: власна розробка авторів

викликає побоювання щодо їх конфіденційності та контролю. Далі необхідно враховувати соціальні та економічні наслідки, до яких може привести диджиталізація шляхом автоматизація та роботизація основних бізнес-процесів. Також необхідно не забувати про виникнення нерівності через розрив між тими, хто має доступ до сучасних технологій, і тими, хто його не має, з часом цей рівень може тільки збільшуватися. Наступна група ризикових факторів запровадження диджиталізації, які виникають через швидкий розвиток технологій та випереджають законодавчі ініціативи, це – правові та регуляторні проблеми. Така ситуація може привести до правових колізій та проблем з регулюванням. Тому, захист прав споживачів у цифровому середовищі, який не можливо здійснити без належним чином підготовленої та оформленої законодавчої бази, має виходити на перший план. Диджиталізація передбачає і культурні зміни, серед яких найзначущі – зміни у способах спілкування. Відбуваються також зміни у способах і засобах спілкування та взаємодії людей, що без сумнівів приведе до соціальних змін, які можуть вплинути на зростання соціальної напруженості. Крім того, постійне зростання обсягів доступної цифрової інформації та постійна присутність у цифровому середовищі можуть викликати стрес, депресію та інші, ще мабуть й не досліджені, проблеми з психічним здоров'ям населення. Останнім, проте не менш значущим, наслідком запровадження диджиталізації є кібербезпека. Збільшення кількості даних у цифровому форматі робить їх більш привабливою метою для зловмисників. Використовуючи певні вразливості програмного забезпечення, зловмисники можуть отримати доступ до вразливих конфіденційних даних як окремих фізичних осіб, так і цілих організацій, як комерційних так і державних. Ці дані можуть бути оприлюдненні, використані для збагачення чи просто знищені (навіть разом із обладнанням, на якому використовується вразливе програмне забезпечення). Отриманий кіберзлочинцями доступ до програмного забезпечення, може бути використаний для спостереження та контролю за користувачами. У будь-якому разі, негативні наслідки від зазначених дій важко піддаються прогнозуванню та оцінці.

Важливість питання кібербезпеки підтверджують приклади відомих кібератак, що відбулись за першу чверть XXI сторіччя (табл. 1).

Таблиця 1

Відомі кібератаки XXI сторіччя

№	Рік	Назва	Опис	Наслідки
1	2	3	4	5
1	2007	TJX Companies Data Breach [8]	Витік даних клієнтів роздрібної мережі	Скомпрометовано дані 94 мільйонів кредитних та дебетових карток
2	2008	Heartland Payment Systems [9]	Витік даних із системи обробки платежів	Скомпрометовано дані 130 мільйонів кредитних та дебетових карток
3	2009	Operation Aurora [10]	Серія атак на великі компанії, включаючи Google та Adobe	Витік інтелектуальної власності та конфіденційної інформації
4	2009–2010	Stuxnet [11]	Черв'як, націлений на іранські ядерні об'єкти	Пошкоджено близько 1000 центрифуг для збагачення урану
5	2011	RSA Security Breach [12]	Злом системи безпеки компанії RSA	Скомпрометовані дані про двофакторну аутентифікацію
6	2013	Target Data Breach [13]	Витік даних про кредитні та дебетові картки	Скомпрометовані дані близько 40 мільйонів карток
7	2013	Adobe Data Breach [14]	Витік даних користувачів та вихідного коду програмного забезпечення	Скомпрометовано дані 38 мільйонів користувачів
8	2013–2014	Yahoo Data Breaches [15]	Два великі витоку даних, що торкнулися більше 3 мільярдів користувачів	Значні фінансові та репутаційні втрати
9	2014	Sony Pictures Hack [16]	Хакерська атака, ймовірно пов'язана з Північною Кореєю	Витік конфіденційної інформації, включаючи фільми та особисті дані співробітників
10	2014	Mt. Gox Hack [17]	Злам найбільшої біржі біткоїнів	Втрата близько 850 тисяч біткоїнів
11	2014	eBay Data Breach [18]	Витік даних користувачів аукціонного сайту	Скомпрометовано дані 145 мільйонів користувачів
12	2015	Anthem Inc. Data Breach [19]	Витік даних із найбільшої страхової компанії	Скомпрометовано дані 80 мільйонів клієнтів
13	2015	Ashley Madison Hack [20]	Зламування сайту знайомств для одружених людей	Витік особистих даних мільйонів користувачів
14	2015	Office of Personnel Management Data Breach [21]	Витік даних співробітників федерального уряду США	Скомпрометовано дані 21.5 мільйонів осіб
15	2016	Uber Data Breach [22]	Витік даних користувачів сервісу таксі	Скомпрометовано дані 57 мільйонів користувачів та водіїв

Продовження Таблиці 1

1	2	3	4	5
16	2016	DNC Email Leak [23]	Витік електронних листів Національного комітету Демократичної партії США	Значний вплив на політичний ландшафт США
17	2017	WannaCry [24]	Вірус-вимагач, який використовує вразливість у Windows для шифрування файлів та вимоги викупу	Заражено понад 200 тисяч комп'ютерів у 150 країнах
18	2017	NotPetya [25]	Вірус-вимагач, який маскувався під програму для шифрування даних	Пошкоджено безліч компаній, включаючи Maersk, Merck та FedEx, зі збитками в мільярди доларів
19	2017	Equifax Data Breach [26]	Витік даних із великої кредитної компанії	Скомпрометовано особисті дані 147 мільйонів осіб
20	2018	Marriott International Data Breach [27]	Витік даних клієнтів мережі готелів	Скомпрометован дані 500 мільйонів гостей.
21	2020	SolarWinds Hacker Attack [28]	Атака використовувала вразливість в оновленні програмного забезпечення SolarWinds Orion, що дозволило хакерам впровадити шкідливий код в систему	Вразливість торкнулася більше 18 000 організацій, включаючи Міністерство внутрішньої безпеки та державні установи США. Хакери отримали доступ до чутливих даних
22	2021	Microsoft Exchange Server Data Breach [29]	Уразливості Microsoft Exchange Server дозволили хакерам (угруповання Hafnium) отримати віддалений доступ до поштових скриньок і даних	Атака торкнулася десятків тисяч організацій по всьому світу. Microsoft випустила термінові патчі для захисту від атаки
23	2021	Colonial Pipeline Ransomware Attack [30]	Хакери з угруповання DarkSide провели атаку програм-вимагачів, зашифрувавши дані та вимагаючи викупу	Атака призвела до закриття найбільшого трубопроводу в США, спричинивши дефіцит палива на східному узбережжі та подорожчання цін
24	2021	Facebook Data Breach [31]	Витік даних стосувався понад 500 мільйонів користувачів Facebook, включаючи номери телефонів та особисті дані	Дані були опубліковані на форумах хакерів, що збільшило ризик фішингу та інших атак на користувачів
25	2021	Kaseya VSA Ransomware Attack [32]	Уразливості програмного забезпечення для управління IT-інфраструктурою Kaseya використовувалися для атак на 1500 компаній через постачальників IT-послуг	Хакери з REvil зажадали понад 70 мільйонів доларів у вигляді викупу. Безліч компаній зіткнулися з простоями та витоками даних
26	2022	Uber Data Breach [33]	Хакери отримали доступ до внутрішніх систем Uber, включаючи бази даних із особистими даними користувачів та водіїв	Витік викликав громадську занепокоєння щодо безпеки особистої інформації та спричинив розслідування з боку регулюючих органів
27	2023	MOVEit Transfer Data Breach [34]	Вразливість у MOVEit призвела до масових витоків даних від багатьох організацій, включаючи фінансові та медичні установи	Хакери із Clop використовували вразливість для крадіжки конфіденційної інформації, що вплинуло на репутацію багатьох компаній

Джерело: складено авторами за матеріалами [8–34]

Звісно, що це далеко не повний перелік кіберзлочинів, які були скоєні за останні 20–25 років, своїм успіхом вони завдячують низці проблем із кібербезпекою, що наведено у табл. 2.

Таблиця 2

Ймовірні причини успіху кібератак

№	Причина	Приклад	Опис
1	2	3	4
1	Вразливості у програмному забезпеченні	WannaCry [24], NotPetya [24]	Використання відомих уразливостей, для яких існували патчі, але організації не встигли або не захотіли їх впровадити
		Microsoft Exchange Server [29], SolarWinds [28]	Використання раніше невідомих уразливості, що надавали зловмисникам можливість проникати в системи без виявлення
2	Недостатній рівень безпеки мереж	Heartland Payment Systems [9], TJX Companies [8]	Недостатній захист мережі дозволив зловмисникам проникнути через слабкі місця (незашифровані або погано захищені мережеві протоколи)
		eBay [18], Adobe [14]	Зловмисники отримали доступ до систем через крадіжку облікових даних співробітників

Продовження Таблиці 2

1	2	3	4
3	Соціальна інженерія та фішинг	RSA Security [12], DNC Email Leak [23], Uber [33]	Використання фішингових листів дозволяло зловмисникам отримати доступ до облікових даних співробітників
4	Складність інфраструктури та систем	Yahoo [15], Marriott International [27] Target [13], Sony Pictures [16]	Наявність дуже складних IT-систем ускладнило своєчасне виявлення й виправлення вразливостей Відсутність чіткої ізоляції критичних систем від менш важливих частин мережі
5	Недостатнє шифрування та управління даними	Anthem Inc. [19], Office of Personnel Management [21] Uber [22], Ashley Madison [20]	Дані зберігалися без належного рівня шифрування Зловмисники використали слабкі або скомпрометовані паролі
6	Масштаб і складність атак	SolarWinds []28, Kaseya VSA []32 Colonial Pipeline [30]	Зловмисники атакували постачальників програмного забезпечення або інфраструктури, які мали доступ до великої кількості клієнтів Зловмисники застосовували розподілені атаки (DDoS) для паралізації систем
7	Неналежна відповідь на атаки	Uber [33] Target [13], Equifax [26]	Компанія не одразу повідомила про злам і намагалася приховати атаку, що дозволило зловмисникам продовжувати свої дії і збільшило збитки Компанії не мали адекватного плану дій на випадок кібератак, що ускладнило швидке реагування та мінімізацію шкоди
8	Політичні та геополітичні мотиви	Operation Aurora [10], Stuxnet [11], Sony Pictures [16]	Спричинені або підтримані державними діячами з метою шпигунства або нанесення шкоди певним країнам чи корпораціям
9	Відсутність кібергігієни у користувачів	RSA Security [12], DNC Email Leak [23], Uber [22], Ashley Madison [20]	Недостатня кібергігієна та недбалість користувачів дозволила зловмисникам використовувати фішинг та соціальну інженерію для компрометації систем

Джерело: складено авторами за матеріалами [8–34]

Успішність більшості кібератак була обумовлена поєднанням технічних вразливостей, людських помилок та недостатньої безпеки мереж і систем. Організаціям необхідно впроваджувати багаторівневі заходи безпеки, включаючи постійне оновлення систем, навчання працівників і забезпечення шифрування та сегментації мережі, для запобігання подібним інцидентам у майбутньому. Крім того, зрозуміло, що проблема кібербезпеки актуальна не лише для індивідуальних користувачів, а навіть для великих підприємств та держав. Притаманною вона є навіть для великих «гравців» ринку інформаційних технологій. Впевнено можна стверджувати, що диджиталізація, яка надає нові можливості передбачає і нові виклики з кібербезпеки, які й надалі будуть лише зростати.

Для мінімізації ризиків, пов'язаних з кіберзагрозами, необхідні комплексні заходи, що включають але не обмежуються діями, що перелічені у табл. 3.

Таблиця 3

Комплексна система заходів щодо посилення кібербезпеки

№ з/п	Захід	Сутність	Очікуваний результат
1	2	3	4
1	Навчання та підвищення обізнаності персоналу	Проведення регулярних тренінгів та семінарів з питань кібербезпеки для співробітників	Підвищення рівня знань і уважності користувачів програмних засобів, що зменшує ризик людських помилок та успішності фішингових атак
2	Розробка та впровадження політик забезпечення безпеки інформації	Створення комплексу документів, що визначають правила та процедури захисту інформаційних ресурсів організації та/або держави	Чітко встановлені стандарти безпеки, які сприяють зниженню ймовірності порушень та забезпечують послідовність дій у разі інцидентів
3	Впровадження систем управління доступом до інформаційних систем підприємства	Використання інструментів та процесів для контролю та моніторингу доступу до інформаційних систем та даних	Забезпечення того, що лише авторизовані користувачі мають доступ до відповідних ресурсів, що суттєво мінімізує можливість несанкціонованого доступу
4	Використання антивірусного та антишпигунського програмного забезпечення	Встановлення та регулярне оновлення захисних програм для виявлення та нейтралізації шкідливого програмного забезпечення	Захист систем від вірусів, шпигунського програмного забезпечення та інших загроз, що забезпечує стабільність та безпеку роботи підприємства

Продовження Таблиці 3

1	2	3	4
5	Регулярне оновлення систем програмного забезпечення	Постійне встановлення оновлень та патчів для операційних систем, програмного забезпечення та апаратних засобів.	Усунення відомих вразливостей, що запобігає можливим атакам через експлуатацію недоліків безпеки
6	Своєчасне резервне копіювання даних	Створення регулярних резервних копій важливих даних та їх зберігання у безпечних місцях	Можливість відновлення інформації у разі втрати даних через атаки, технічні збої або інші інциденти
7	Використання шифрування	Захист даних шляхом їх кодування як під час передачі, так і при зберіганні	Забезпечення конфіденційності інформації, що унеможливлює доступ до неї неавторизованих осіб
8	Проведення аудиту та тестування безпеки	Регулярна оцінка стану кібербезпеки через аудити, пенетраційні тести та оцінку вразливостей	Виявлення слабких місць у системах захисту та своєчасне їх усунення з метою підвищення загального рівня безпеки
9	Впровадження систем виявлення та реагування на інциденти	Використання інтегрованих рішень для моніторингу, аналізу та реагування на кіберінциденти в режимі реального часу	Швидке виявлення та ефективне реагування на загрози, що зменшує можливі збитки від атак
10	Формування системи управління ризиками та оцінка рівня безпеки	Систематичний підхід до ідентифікації, оцінки та управління ризиками, пов'язаними з кібербезпекою	Збалансований підхід до захисту інформаційних ресурсів, що дозволяє ефективно розподіляти ресурси та пріоритети для мінімізації ризиків.
11	Розробка та імплементація відповідних законодавчих та нормативних актів, що регулють питання кібербезпеки	Розробка на державному рівні нормативних актів, які регулюють питання кібербезпеки, захисту даних та відповідальності за порушення у сфері цифрових технологій	Забезпечення правової основи для захисту інформаційних ресурсів, встановлення чітких правил для організацій та користувачів, підвищення рівня відповідальності за кіберзлочинами

Джерело: власна розробка

Системне запровадження цих заходів, включаючи розробку відповідного законодавства, сприятиме створенню надійної кібербезпекової інфраструктури, яка підтримуватиме та стимулюватиме розвиток диджиталізації не тільки на рівні підприємств, а й на національному рівні. Завдяки комплексним заходам, що включають законодавче регулювання, фінансову підтримку, освітні ініціативи та міжнародну співпрацю, держава може створити сприятливі умови для безпечної диджиталізації. Це не лише захищає інформаційні ресурси та інфраструктуру, але й сприяє довірі громадян та бізнесу до цифрових технологій, що є основою для сталого розвитку в умовах сучасного інформаційного суспільства.

Висновки. Отже, необхідно зазначити, що диджиталізація є потужним інструментом сучасного розвитку суспільства, що забезпечує значні переваги для економіки, бізнесу та суспільства в цілому. Впровадження цифрових технологій сприяє автоматизації процесів, підвищенню ефективності діяльності, покращенню якості послуг та створенню нових можливостей для інновацій. Україна активно використовує цифрові рішення для розвитку різних секторів, включаючи державне управління, освіту, охорону здоров'я та фінансові послуги, що сприяє підвищенню прозорості, доступності та конкурентоспроможності національної економіки. Однак, разом із численними перевагами, диджиталізація приносить і низку серйозних викликів, серед яких ключовим є питання кібербезпеки. Зі зростанням обсягів оброблюваних та зберігаємих даних зростає й кількість кіберзагроз, таких як витоки інформації, хакерські атаки, фішингові кампанії та інші форми кіберзлочинності. Недостатня увага до питань кібербезпеки може значно ускладнити процес цифрової трансформації, створюючи ризики для безпеки даних, конфіденційності інформації та стабільності бізнес-процесів. Відсутність комплексної стратегії кібербезпеки, недостатнє фінансування, низький рівень обізнаності серед громадян та слабка нормативно-правова база є основними перешкодами для забезпечення безпечної диджиталізації в Україні.

Таким чином, для успішної реалізації процесів цифровізації в Україні необхідно комплексно підходити до питань кібербезпеки, включаючи розробку та впровадження ефективних політик, інвестування в захисну інфраструктуру, навчання та підвищення обізнаності персоналу та населення, а також створення сприятливої законодавчої бази. Це дозволить не лише мінімізувати ризики, але й забезпечити сталий розвиток цифрових технологій, підвищуючи загальну ефективність та конкурентоспроможність української економіки в майбутньому. У подальших дослідження автори зосередять свою увагу на стратегічному плануванні заходів щодо забезпечення кібербезпеки та можливостей їх адаптування до специфіки українського ринку.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Лапін А. В., Грінчук І. О., Оленюк Д. О. Діджиталізація економіки в Україні: сучасний стан та перспективи. *Ефективна економіка*. 2022. № 7. URL: https://doi.org/10.32702/2307-2105.2022.7.22 (дата звернення: 25.11.2024).

2. Шлайфер М., Тодощук А. Діджиталізація економіки України в умовах євроінтеграції. *Економіка та суспільство*. 2022. № 45. URL: https://doi.org/10.32782/2524-0072/2022-45-10 (дата звернення: 25.11.2024).

3. Саврас І. З., Фединець Н. І. Цифровізація та інноваційний розвиток підприємства: тенденції, проблеми та перспективи. *Вісник Львівського торговельно-економічного університету*. 2024. № 74. С. 108–114. URL: https://doi.org/10.32782/2522-1205-2023-74-14 (дата звернення: 25.11.2024).

4. Водянка Л. Д., Стахова Н. П. Цифровізація як сучасний фактор розвитку інтелектуального бізнесу. *Ефективна економіка*. 2023. № 7. URL: https://doi.org/10.32702/2307-2105.2023.7.29 (дата звернення: 25.11.2024).

5. Данилишин В. І., Синиця С. М. Діджиталізація на ринку фінансових послуг: сутність та значення для економіки України в умовах сьогодення. Трансформаційна економіка. 2023. № 3 (03). С. 16–20. URL: https://doi.org/10.32782/2786-8141/2023-3-3 (дата звернення: 25.11.2024).

6. Небога Т. В., Лабунська О. Б. Діджиталізація суб'єктів бізнесу національної економіки. *Цифрова економіка та економічна безпека*. 2023. № 5. С. 9–19. URL: https://doi.org/10.32782/dees.5-2 (дата звернення: 25.11.2024).

7. Діджиталізація в Україні: електронне врядування та держпослуги. URL: http://week.dp.gov.ua/osvitnia-prohrama/pislya91/digitalizaciya-v-ukraini (дата звернення: 25.11.2024).

8. Covert E. Case study: TJ maxx's data breach. *Medium.* URL: https://medium.com/@edwincovert/case-study-tjx-data-breach-4ace4cc2732a (accessed: 25.11.2024).

9. Lewis D. Heartland payment systems suffers data breach. *Forbes*. URL: https://www.forbes.com/sites/davelewis/2015/05/31/heartland-payment-systems-suffers-data-breach (accessed: 25.11.2024).

10. Operation aurora – 2010's major breach by chinese hackers. *Exabeam.* URL: https://www.exabeam.com/blog/infosec-trends/operation-aurora-2010s-major-breach-by-chinese-hackers/ (accessed: 25.11.2024).

11. Fruhlinger J. Stuxnet explained: the first known cyberweapon. *CSO Online*. URL: https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html (accessed: 25.11.2024).

12. Vignesh. Email breach chronicles: RSA's infiltration–the spear phishing incident of 2011. *Zoho Workplace*. URL: https://www.zoho.com/workplace/articles/rsa-spear-phishing-attack.html (accessed: 25.11.2024).

13. Jones C. Warnings (& lessons) of the 2013 target data breach. Technology Decisions Aren't Black and White. Think Red. URL: https://redriver.com/security/target-data-breach (accessed: 25.11.2024).

14. What happened in the Adobe data breach? Twingate: It's time to ditch your VPN. *Twingate*.URL: https://www.twingate.com/blog/tips/adobe-data-breach (accessed: 25.11.2024).

15. BPB Online. Yahoo data breach: what actually happened?. *Medium*. URL: https://bpbonline.medium.com/yahoo-data-breach-what-actually-happened-54cf8f3f7c93 (accessed: 25.11.2024).

16. Cyber case study: sony pictures entertainment hack – coverlink insurance – ohio insurance agency. CoverLink Insurance – Ohio Insurance Agency. URL: https://coverlink.com/case-study/sony-pictures-entertainment-hack (accessed: 25.11.2024).

17. Trust Wallet. The story of mt. gox: explained. *Trust Blog*. URL: https://trustwallet.com/blog/mt-gox-explained (accessed: 25.11.2024).

18. Brodowicz M. Cyber attack on ebay company: the summer of 2014 report. *Aithor.com*. URL: https://aithor.com/essay-examples/cyber-attack-on-ebay-company-the-summer-of-2014-report (accessed: 25.11.2024).

19. Consumer information on Anthem Blue Cross data breach. *CA Department of Insurance*. URL: https://www.insurance.ca.gov/0400-news/0100-press-releases/anthemcyberattack.cfm (accessed: 25.11.2024).

20. Eidell L. What happened to ashley madison? The true story of the dating site's infamous 2015 hack – and how it bounced back. *People.com.* URL: https://people.com/ashley-madison-dating-website-2015-hack-true-story-8644849 (accessed: 25.11.2024).

21. Office of Personnel Management data breach (2015) – International cyber law: interactive toolkit. *International cyber law: interactive toolkit*. URL: https://cyberlaw.ccdcoe.org/wiki/Office_of_Personnel_Management_data_breach_(2015) (accessed: 25.11.2024).

22. Uber breach exposes the data of 57 million drivers and users | trend micro (GB). Trend Micro (DE). *Branchenführende KI-Cybersicherheitsplattform*. URL: https://www.trendmicro.com/vinfo/gb/security/news/cybercrime-and-digital-threats/uber-breach-exposes-the-data-of-57-million-drivers-and-users (accessed: 25.11.2024).

23. How the Russians hacked the DNC and passed its emails to WikiLeaks. *The Washington Post*. URL: https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html (accessed: 25.11.2024).

24. What was WannaCry? *Malwarebytes*. URL: https://www.malwarebytes.com/wannacry (accessed: 25.11.2024).

25. NotPetya: understanding the destructiveness of cyberattacks – security outlines. *Security Outlines – česko-slovenský portál o bezpečnosti*. URL: https://www.securityoutlines.cz/notpetya-understanding-the-destructiveness-of-cyberattacks/ (accessed: 25.11.2024).

26. Equifax data breach settlement. *Federal Trade Commission*. URL: https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement (accessed: 25.11.2024).

27. Cyber case study: marriott data breach – coverlink insurance – ohio insurance agency. CoverLink Insurance – Ohio Insurance Agency. URL: https://coverlink.com/case-study/marriott-data-breach (accessed: 25.11.2024).

28. Kerner S. M., Oladimeji S. SolarWinds hack explained: everything you need to know. WhatIs. URL: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know (accessed: 25.11.2024).

29. Microsoft Exchange Server data breach (2021) International cyber law: interactive toolkit. International cyber law. *Interactive toolkit*. URL: https://cyberlaw.ccdcoe.org/wiki/Microsoft_Exchange_Server_data_breach_(2021) (accessed: 25.11.2024).

30. The attack on colonial pipeline: what we've learned & what we've done over the past two years. *Cybersecurity and Infrastructure Security Agency CISA*. URL: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years (accessed: 25.11.2024).

31. What happened in the Facebook data breach? Twingate: It's time to ditch your VPN. *Twingate*. URL: https://www.twingate.com/blog/tips/facebook-data-breach (accessed: 25.11.2024).

32. Kaseya VSA ransomware attack (2021) – International cyber law: interactive toolkit. International cyber law. *Interactive toolkit*. URL: https://cyberlaw.ccdcoe.org/wiki/Kaseya_VSA_ransomware_attack_(2021) (accessed: 25.11.2024).

33. What caused the uber data breach in 2022? Third-Party Risk and Attack Surface Management Software. *UpGuard*. URL: https://www.upguard.com/blog/what-caused-the-uber-data-breach (accessed: 25.11.2024).

34. MOVEit transfer data breaches Deep Dive. Operational Risk Management in Financial Services. *ORX*. URL: https://orx.org/resource/moveit-transfer-data-breaches (accessed: 25.11.2024).

REFERENCES:

1. Lapin A. V., Hrinchuk I. O., Oleniuk D. O. (2022) Didzhytalizatsiia ekonomiky v Ukraini: suchasnyi stan ta perspektyvy [Digitalization of the economy in Ukraine: current state and prospects]. *Efektyvna ekonomika*, vol. 7. Available at: https://doi.org/10.32702/2307-2105.2022.7.22 (accessedNovember 25, 2024)

2. Shlaifer M., Todoshchuk A. (2022) Didzhytalizatsiia ekonomiky ukrainy v umovakh yevrointehratsii. [Digitalization of the Ukrainian economy in the context of European integration]. *Ekonomika ta suspilstvo*, vol. 45. Available at: https://doi.org/10.32782/2524-0072/2022-45-10 (accessedNovember 25, 2024)

3. Savras I. Z., Fedynets N. I. (2024) Tsyfrovizatsiia ta innovatsiinyi rozvytok pidpryiemstva: tendentsii, problemy ta perspektyvy [Digitalisation and innovative development of the enterprise: trends, challenges and prospects]. *Visnyk Lvivskoho torhovelno-ekonomichnoho universytetu*, vol. 74, pp. 108–114. Available at: https://doi.org/10.32782/2522-1205-2023-74-14 (accessedNovember 25, 2024)

4. Vodianka L. D., Stakhova N. P. (2023) Tsyfrovizatsiia yak suchasnyi faktor rozvytku intelektualnoho biznesu. [Digitalization as a modern factor in the development of intellectual business]. *Efektyvna ekonomika*, vol. 7. Available at: https://doi.org/10.32702/2307-2105.2023.7.29 (accessedNovember 25, 2024)

5. Danylyshyn V. I., Synytsia S. M. (2023) Didzhytalizatsiia na rynku finansovykh posluh: sutnist ta znachennia dlia ekonomiky Ukrainy v umovakh sohodennia. [Digitalization in the financial services market: essence and significance for the economy of Ukraine in today's conditions]. *Transformatsiina ekonomika*, vol. 3, pp. 16–20. Available at: https://doi.org/10.32782/2786-8141/2023-3-3 (accessedNovember 25, 2024)

6. Neboha T. V., Labunska O. B. (2023) Didzhytalizatsiia subiektiv biznesu natsionalnoi ekonomiky. [Digitalization of business entities of the national economy]. *Tsyfrova ekonomika ta ekonomichna bezpeka*, vol. 3, pp. 9–19. Available at: https://doi.org/10.32782/dees.5-2 (accessedNovember 25, 2024)

7. Didzhytalizatsiia v Ukraini: elektronne vriaduvannia ta derzhposluhy. [Digitalization in Ukraine: e-government and public services]. Available at: http://week.dp.gov.ua/osvitnia-prohrama/pislya91/digitalizaciya-v-ukraini (accessedNovember 25, 2024)

8. Covert E. Case study: TJ maxx's data breach. *Medium.* Available at: https://medium.com/@edwincovert/case-study-tjx-data-breach-4ace4cc2732a (accessed: 25.11.2024).

9. Lewis D. (2015) Heartland payment systems suffers data breach. *Forbes.* Available at: https://www.forbes.com/sites/davelewis/2015/05/31/heartland-payment-systems-suffers-data-breach (accessed: 25.11.2024).

10. Operation aurora – 2010's major breach by chinese hackers. *Exabeam*. Available at: https://www.exabeam.com/blog/infosec-trends/operation-aurora-2010s-major-breach-by-chinese-hackers/ (accessed: 25.11.2024).

11. Fruhlinger J. Stuxnet explained: the first known cyberweapon. *CSO Online*. Available at: https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html (accessed: 25.11.2024).

12. Vignesh. Email breach chronicles: RSA's infiltration–the spear phishing incident of 2011. *Zoho Workplace*. Available at: https://www.zoho.com/workplace/articles/rsa-spear-phishing-attack.html (accessed: 25.11.2024).

13. Jones C. Warnings (& lessons) of the 2013 target data breach. Red River | Technology Decisions Aren't Black and White. Think Red. Available at: https://redriver.com/security/target-data-breach (accessed: 25.11.2024).

14. What happened in the Adobe data breach? Twingate: It's time to ditch your VPN. Available at: https://www.twingate.com/blog/tips/adobe-data-breach (accessed: 25.11.2024).

15. BPB Online. Yahoo data breach: what actually happened?. *Medium*. Available at: https://bpbonline.medium.com/yahoo-data-breach-what-actually-happened-54cf8f3f7c93 (accessed: 25.11.2024).

16. Cyber case study: sony pictures entertainment hack – coverlink insurance – ohio insurance agency.

CoverLink Insurance – Ohio Insurance Agency. Available at: https://coverlink.com/case-study/sony-pictures-entertainment-hack/ (accessed: 25.11.2024).

17. Trust Wallet. The story of mt. gox: explained. *Trust Blog*. Available at: https://trustwallet.com/blog/mt-gox-explained (accessed: 25.11.2024).

18. Brodowicz M. (2014) Cyber attack on ebay company: the summer of 2014 report. aithor.com. Available at: https://aithor.com/essay-examples/cyber-attack-on-ebay-company-the-summer-of-2014-report (accessed: 25.11.2024).

19. Consumer information on Anthem Blue Cross data breach. *CA Department of Insurance.* Available at: https://www.insurance.ca.gov/0400-news/0100-press-releases/anthemcyberattack.cfm (accessed: 25.11.2024).

20. Eidell L. (2015) What happened to ashley madison? The true story of the dating site's infamous 2015 hack – and how it bounced back. *People.com*. Available at: https://people.com/ashley-madison-dating-website-2015-hack-true-story-8644849 (accessed: 25.11.2024).

21. Office of Personnel Management data breach (2015) – International cyber law: interactive toolkit. International cyber law: interactive toolkit. Available at: https://cyberlaw.ccdcoe.org/wiki/Office_of_Personnel_Management_data_breach_(2015) (accessed: 25.11.2024).

22. Uber breach exposes the data of 57 million drivers and users | trend micro (GB). Trend Micro (DE) | Branchenführende KI-Cybersicherheitsplattform. Available at: https://www.trendmicro.com/vinfo/gb/security/news/cybercrime-and-digital-threats/uber-breach-exposes-the-data-of-57-million-drivers-and-users (accessed: 25.11.2024).

23. How the Russians hacked the DNC and passed its emails to WikiLeaks (2018). *The Washington Post.* Available at: https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html (accessed: 25.11.2024).

24. What was WannaCry? *Malwarebytes.* Available at: https://www.malwarebytes.com/wannacry (accessed: 25.11.2024).

25. NotPetya: understanding the destructiveness of cyberattacks – security outlines. *Security Outlines – česko-slovenský portál o bezpečnosti*. Available at: https://www.securityoutlines.cz/notpetya-understanding-the-destructiveness-of-cyberattacks/ (accessed: 25.11.2024).

26. Equifax data breach settlement. *Federal Trade Commission*. Available at: https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement (accessed: 25.11.2024).

27. Cyber case study: marriott data breach – coverlink insurance – ohio insurance agency. CoverLink Insurance – Ohio Insurance Agency. Available at: https://coverlink.com/case-study/marriott-data-breach (accessed: 25.11.2024).

28. Kerner S. M., Oladimeji S. SolarWinds hack explained: everything you need to know. WhatIs. Available at: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know (accessed: 25.11.2024).

29. Microsoft Exchange Server data breach (2021) *International cyber law: interactive toolkit.* Available at: https://cyberlaw.ccdcoe.org/wiki/Microsoft_Exchange_Server_data_breach_(2021) (accessed: 25.11.2024).

30. The attack on colonial pipeline: what we've learned & what we've done over the past two years. *Cybersecurity and Infrastructure Security Agency CISA*. Available at: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years (accessed: 25.11.2024).

31. What happened in the Facebook data breach? Twingate: It's time to ditch your VPN. Available at: https://www.twingate.com/blog/tips/facebook-data-breach (accessed: 25.11.2024).

32. Kaseya VSA ransomware attack (2021). *International cyber law: interactive toolkit*. Available at: https://cyberlaw.ccdcoe.org/wiki/Kaseya_VSA_ransomware_attack_(2021) (accessed: 25.11.2024).

33. What caused the uber data breach in 2022? Third-Party Risk and Attack Surface Management Software. *UpGuard.* Available at: https://www.upguard.com/blog/what-caused-the-uber-data-breach (accessed: 25.11.2024).

34. MOVEit transfer data breaches Deep Dive. ORX News. Operational Risk Management in Financial Services. *ORX*. Available at: https://orx.org/resource/moveit-transfer-data-breaches (accessed: 25.11.2024).