ЦИФРОВІ ТЕХНОЛОГІЇ

УДК 004.056:004.9
DOI: 10.31617/2.2022(43)04

Юлія БІЛЯВСЬКА
к. е. н., доцент, доцент кафедри менеджменту
Державного торговельно-економічного університету
вул. Кіото, 19, м. Київ, 02156, Україна
y.biliavska@knute.edu.ua

Yuliia BILIAVSKA
PhD (Economics),
Associate Professor, Associate Professor at the Department of Management
State University of Trade and Economics
19, Kyoto St., Kyiv, 02156, Ukraine
ORCID: 0000-0002-8183-4036

Ярослав ШЕСТАК
директор Інформаційно-обчислювального центру Головного центру інформаційних технологій, ст. викладач кафедри програмної інженерії та кібербезпеки
Державного торговельно-економічного університету
вул. Кіото, 19, м. Київ, 02156, Україна
shestack@knute.edu.ua

Yaroslav SHESTAK
Director of the Information and Computing Center of the Main Center of Information Technologies, sen. lecturer at the Department of Software Engineering and Cybersecurity
State University of Trade and Economics
19, Kyoto St., Kyiv, 02156, Ukraine
ORCID: 0000-0002-5102-9642

КІБЕРБЕЗПЕКА ТА КІБЕРГІГІЄНА: НОВА ЕРА ЦИФРОВИХ ТЕХНОЛОГІЙ

Вступ. Цифрові технології – ключовий фактор розвитку підприємств, отже, кібербезпека стає дедалі актуальнішим напрямом наукових досліджень.

Проблема. Розвиток Суспільства 5.0. та перехід на 5*G*-мережі несе нові виклики, пов'язані з коректною роботою програмного забезпечення, де існує безліч кіберзагроз. Особливо важливо українцям дотримуватися вимог кібергігієни в умовах війни.

Метою статті є аналіз змін на ринку цифрових технологій у контексті кібербезпеки й обґрунтування рекомендацій із дотримання кібергігієни в управлінні бізнесом.

Методи. Застосовано комплекс загальнонаукових, спеціальних та специфічних методів історичних, логічних й аналітичних узагаль-

CYBER SECURITY AND CYBER HYGIENE: THE NEW ERA OF DIGITAL TECHNOLOGIES

Introduction. Digital technologies are a key factor in the development of enterprises, so cybersecurity is becoming an increasingly important area of research.

Problem. Development of Society 5.0. and the move to 5G networks brings new challenges to the proper operation of software, where there are many cyber threats. It is especially important for Ukrainians to comply with the requirements of cyber hygiene during the war.

The aim of the article is to analyse the changes in the digital technology market in the context of cybersecurity and substantiate the recommendations for cyber hygiene in business management.

Methods. A set of general scientific, special and specific methods of historical, logical and

Внесок авторів: Білявська Ю. – 50 %, Шестак Я. – 50 %.
Автори не отримували прямого фінансування для цього дослідження.

Biliavska Ju., Shestak Ja. Dovira do cyfrovyh tehnologij: nova era kiberbezpeky. *Mizhnarodnyj naukovo-praktychnyj zhurnal "Tovary i rynky"*. 2022. № 3 (43). S. 47–59. https://doi.org/10.31617/2.2022(43)04

нень; економіко-статистичних (порівняльний аналіз, спостереження, а також групування на основі використання програмних продуктів *MS Excel*); діалектичний, абстрактно-логічний і системний аналіз.

Результати дослідження. Кібербезпека здатна не лише реагувати на інциденти, але й запобігати атакам до їх початку. З метою покращення ефективності діяльності підприємства керівники з кібербезпеки сфокусовані на технологіях, а також на тісній співпраці з бізнес-командами. Результатом такої взаємодії є готовність кібербезпеки боротися зі зловмисниками на рівних, даючи відсіч і відбиваючи атаки з небаченою раніше результативністю.

Висновки. Досвід тривалої роботи у дистанційному режимі вніс довгострокові зміни в політику корпоративної кібербезпеки підприємства. Щоб зменшити ймовірність і мінімізувати наслідки порушення кібербезпеки, підприємства мають шукати для себе шляхи спрощення заходів щодо неї. Це гарантує, що кібербезпека стане стимулом для розвитку бізнесу, а не перешкодою наявним і майбутнім планам.

Ключові слова: цифровізація, цифрова технологія, кіберуправління бізнесом, кібербезпека, кібератака, кіберризик, кібергігієна, пандемія *COVID*-19.

analytical generalizations has been applied; economic and statistical (comparative analysis, observation, as well as grouping based on the use of MS Excel software products); dialectical, abstract-logical and systematic analysis.

Results. Cybersecurity can not only respond to incidents, but also prevent attacks before they occur. In order to improve the efficiency of the enterprise, cybersecurity managers focus on technology, as well as on close cooperation with business teams. The result of this interaction is the readiness of cybersecurity to fight criminals on an equal footing, repelling attacks with unprecedented effectiveness.

Conclusions. The experience of long-term work in the remote mode has made long-term changes in the corporate cybersecurity policy of the enterprise. To reduce the likelihood and minimize the consequences of cybersecurity violation, businesses need to find ways to simplify measures for it. This ensures that cybersecurity is a stimulus for business development, not an obstacle to existing and future plans.

Keywords: digitalization, digital technology, cyber business management, cybersecurity, cyberattack, cyber risk, cyber hygiene, pandemic *COVID*-19.

JEL Classification: M20, M21, M59, C80

Вступ. Цифрові технології нині є ключовим фактором розвитку підприємств, отже, кібербезпека стає дедалі актуальнішим напрямом наукових досліджень. Розвиток Суспільства 5.0. та перехід на 5*G*-мережі зумовлює нові виклики, які беззаперечно пов'язані з коректною роботою програмного забезпечення, активне користування яким, своєю чергою, несе кіберзагрози. Саме тому поняття кібербезпеки постійно розширюється паралельно із диджиталізацією суспільства.

Проблема. Значну частину персоналу підприємств в усьому світі переведено в режим дистанційної роботи внаслідок пандемії *COVID*-19, а тому необхідно беззаперечно стежити за обізнаністю ризиків, які пов'язані з віддаленою роботою: атаками на акаунти в соціальних мережах; незахищеним віддаленим підключенням до установи; спробами фішингових атак; поширеним використанням офісної техніки в особистих цілях; шахрайством та незахищеністю інформаційних даних. Електронні підписи та послуги електронної ідентифікації є двома з основних рішень, які прискорюють цифрову взаємодію між учасниками, наприклад, для підтвердження особи під час доступу до державних послуг або підписання юридичних контрактів.

Глобальне опитування серед інвесторів, аналітиків та керівників підприємств свідчить про те, що кібератаки є найбільш серйозною поміж інших значних загроз для бізнесу, як-от геополітична нестабільність, темпи технологічних змін, популізм та протекціонізм. Більшість потенційних інвесторів вважають за необхідне в управлінні бізнесом зосередитися на питаннях кібербезпеки, кіберуправління, щоб підвищити довіру клієнтів до своєї діяльності.

Сьогодні, коли країна перебуває в умовах воєнного стану, не лише для ІТ-фахівців, але й для будь-якого громадянина важливими є цифрова грамотність, дотримання цифрового етикету та правил кібергігієни. З початком війни ІТ-фахівці з усієї країни долучилися до кіберполіції та зуміли дати відсіч агресору. В результаті злагоджених дій були виведені з ладу критично важливі інформаційні системи окупанта. Проте і пересічним українцям необхідно дотримуватися вимог кібергігієни, оскільки інформаційний простір активно використовується ворогом для поширення фейків, дипфейків, підробки сайтів, фішингових атак, заволодіння акаунтами тощо.

Аналіз останніх досліджень і публікацій. Теоретичні та практичні аспекти розвитку цифрових технологій завжди в полі зору вчених різних галузей знань і наукових шкіл. Так, Г. М. Дергачова і Я. О. Колешня [1] обґрунтували цифрову трансформацію як зміну форми діяльності підприємств, перебудову організаційної структури, застосування нових бізнес-моделей, нових джерел та форм отримання доходу, залучення ширшого кола споживачів, виведення їх обслуговування на новий рівень, змішування сфер функціонування у нових форматах бізнес-структур, у т. ч. у вигляді цифрових платформ, а також процес переходу від оптимізації до цифрової економіки.

Питанню цифрових технологій як концепції, що визначає розвиток соціально-економічних систем у контексті домінівного впливу інформації та технологій і ґрунтується на біхевіоральних детермінантах – поведінкових, культурних та соціальних компонентах, присвячено праці C. Chapco-Wade [2] і J. Bloomberg [3]. Організаційні чи суспільні зміни на основі впровадження цифрових технологій розглянуто В. В. Кругловим [4], а В. С. Куйбіда, О. В. Карпенко, В. В. Наместнік [5] переконані, що цифрова трансформація – це спричинені використанням цифрових технологій зміни у природі людини, її мисленні, життєдіяльності й управлінні.

Проблеми інформаційної безпеки знайшли відображення у наукових працях А. І. Марущака [6] та М. В. Гуцалюка [7]. Ефективний механізм правового регулювання щодо протидії кіберзагрозам представлено Д. В. Дубовим [8], А. В. Печенюком [9].

Актуальними є погляди представників бізнесу, які зазначають, що цифрові технології змінюють форми бізнесу в умовах цифрової реальності на основі даних; трансформують методи, а також можливі

способи передачі інформації, забезпечуючи заміну аналогових інструментів на цифрові; цифрові технології застосовуються для зміни моделей управління, а також створення цінності. Вони визначають процес переходу до цифрового бізнесу; докорінне перетворення ділової й організаційної діяльності, процесів, моделей і компетенцій для управління змінами та можливості формування синергії цифрових технологій і стратегії суспільства з урахуванням сьогодення й майбутнього розвитку. Проте сучасна цифрова парадигма світу розвивається у ринкових умовах, що актуалізує комплексний механізм цифрової трансформації управління розвитком бізнесу.

Метою статті є аналіз змін на ринку цифрових технологій у контексті кібербезпеки й обґрунтування рекомендацій з дотримання кібергігієни в управлінні бізнесом.

Методи. Застосовано комплекс загальнонаукових, спеціальних та специфічних методів: історичних, логічних і аналітичних узагальнень – для уточнення категорійного апарату та визначення світових цифрових трендів; економіко-статистичних методів (порівняльний аналіз, спостереження, а також групування на основі використання програмних продуктів *MS Excel*) з метою візуалізації результатів соціологічних досліджень (опитування) для оцінювання довіри представників бізнесу до цифрових технологій. Задля визначення основних позитивних і негативних тенденцій у кібербезпеці застосовано діалектичний, абстрактно-логічний і системний аналіз.

Результати дослідження. Сучасний світ давно зробив перший крок до принципово нової технологічної, економічної та соціальної реальності – епохи цифрової глобалізації. Забезпечення кібербезпеки є одним із вагомих пріоритетів у загальній системі національної безпеки України. Впроваджуючи новітні технології, цивілізація у XXI ст. сприяє активному формуванню супутніх ризиків. Також спостерігаємо зростання питомої ваги кіберзагроз, і ця тенденція в міру розвитку цифрових технологій у поєднанні зі штучним інтелектом лише посилиться, а зростання такого впливу визначатиме формування нової безпекової ситуації. Фундаментом дієвої системи кібербезпеки, безумовно, є ефективна нормативно-правова база, а тому слід зауважити актуальність Указу Президента України "Про рішення Ради національної безпеки і оборони України "Про Стратегію кібербезпеки України" від 26.08.2021 [10], відповідно до якої передбачено перспективи створення максимально вільного та безпечного, відкритого і стабільного кіберпростору в інтересах забезпечення прав людини.

Крім того, в Україні спостерігається постійне зростання довіри до цифрових технологій, оскільки вони лежать в основі розширення конкурентних переваг підприємств, створення нових продуктів та цінностей, а також можливості зміцнювати інноваційні

центри як потужних гравців ринку, так і стартапів. Цифровізація сприяє появі нових ексклюзивних процесів та систем, як, наприклад, цифровий банкінг чи цифрове місто, а в умовах "Індустрії 4.0" у промисловості дедалі більше набувають актуальності кібервиробництво, кібермашини та кіберсистеми. На *рис. 1* представлено ключові цифрові тренди у світі станом на 2022 р.

Рис. 1. Ключові цифрові тренди у світі станом на 2022 р.

Джерело: [11].

Отже, розвиток цифрових трендів, який беззаперечно залежить від цифрових технологій, дедалі більше потребуватиме заходів із кібербезпеки. В умовах диджиталізації світ працює за новими підходами, навіть перебуваючи поза офісом упродовж тривалого часу, працівники можуть продуктивно й ефективно виконувати функціональні обов'язки та постійно залишаються на зв'язку завдяки цифровим технологіям. Існує ймовірність, що такий стиль роботи назавжди залишиться актуальним як для офісних, так і для віддалених працівників. Відтак, працівники та їхні роботодавці матимуть ширші можливості вибору й гнучкості у бізнесі.

Такі раптові зміни в умовах пандемії *COVID*-19 також створили низку проблем щодо кібербезпеки: ведення бізнесу в абсолютно нових умовах у кіберпросторі та захист цифрових даних у більших масштабах, ніж будь-коли в минулому. Такі особливості пов'язані з тим, що працівники приєднують пристрої з офісу до мереж *Wi-Fi* вдома або сторонніх зовнішніх мереж, а також використовують власні персональні пристрої для підключення у хмарі. Така ситуація створює навантаження на ІТ-команди, а також команди безпеки, які мають надавати швидку підтримку у роботі віддаленим працівникам та їхнім при-

строям з метою відсутності будь-якого ризику щодо безпеки. Таким чином, в умовах онлайн-роботи інструменти контролю передбачають супровід працівника не лише в офісі, як це було раніше, а сучасні кіберзлочинці ще більше фокусуються на фішингових атаках, щоб, скориставшись довірою користувачів, викрасти інформацію, скомпрометувати нові системи для віддаленої роботи за допомогою шкідливого програмного забезпечення.

З огляду на особливості розвитку цифровізації останнім часом почастішало використання терміна *"кібергігієна"*. Він не має офіційного трактування, оскільки не закріплений на законодавчому рівні, проте саме під ним розуміється прищеплення і застосування навичок особистої інформаційної безпеки користувачами інформаційно-комунікаційної мережі Інтернет. Ключовою тематикою наукових, науково-технічних та інноваційних конференцій, симпозіумів і форумів як державного, так і міжнародного рівнів є тематика інформаційної безпеки особистості, підприємств та держави. Підприємства готуються до постпандемічного функціонування, і зрозуміло, що співробітники надалі сподіватимуться на гнучкий графік та можливість віддалено працювати, враховуючи той факт, що відбувається певна еволюція і життя не повернеться на етап до пандемії *COVID*-19. Підприємницька діяльність завжди перебуває під загрозою кібератак від початку незалежності країни, а в умовах повномасштабного вторгнення на територію України це набуло промислових масштабів. Відтак, кожне підприємство та суспільство в цілому мають оцінювати вразливість своїх критичних сервісів до інцидентів кібербезпеки й технологічних збоїв. Ці загрози можуть виникати внаслідок атак на системи та інфраструктуру, а можуть бути й наслідками воєнних дій.

Кібербезпека здатна не лише реагувати на інциденти, але й запобігати атакам до їх початку, застосовуючи різні технології та накопичені знання. З метою збільшення ефективності діяльності підприємства керівники з кібербезпеки сфокусовані на технологіях, а також тісній співпраці з бізнес-командами. Результатом такої взаємодії є готовність кіберуправління боротися зі зловмисниками на рівних, даючи відсіч і відбиваючи атаки з небаченою раніше результативністю. Керівники підприємств дедалі частіше звертаються до фахівців з інформаційної безпеки за допомогою у питаннях підвищення стійкості інформаційної системи та створення цінності захисту для бізнесу.

З метою визначення ролі цифрових технологій, кібербезпеки та кібергігієни, враховуючи стрімкий розвиток диджиталізації та наслідки пандемії *COVID*-19, проведено онлайн-опитування 217 респондентів із 45 підприємств України різної форми власності та сфери діяльності. Кожен з них оцінював, як вплинула пандемія *COVID*-19 на кібербезпеку їхнього підприємства. Результати опрацювання анкет уможливили дати відповіді на такі питання: які зміни можуть статися

внаслідок пандемії *COVID*-19; якою має бути роль директора з інформаційної безпеки на підприємстві; яких успіхів досягло підприємство у сфері кібербезпеки за останні три роки; які навички мають бути притаманні фахівцю з кібербезпеки, а також як саме зміниться бюджет підприємства на кібербезпеку у 2022 році. Узагальнені результати проведеного анкетування представлено у *табл. 1*.

Таблиця 1

Аналіз результатів анкетування "Довіра до цифрових технологій"

Питання	Відповідь	Кількість опитаних	% відповідей
Які з наступних змін можуть статися у вашій галузі внаслідок пандемії COVID-19?	Прискорена автоматизація для зниження витрат	35	16.13
	Більш ретельна та детальна кількісна оцінка кіберризиків	40	18.43
	Кібербезпека та конфіденційність даних враховуються у кожному бізнес-рішенні	26	11.98
	Ретельніша взаємодія між директором з інформаційної безпеки, генеральним директором та радою директорів	69	31.80
	Всебічне тестування кіберстійкості підприємства з урахуванням малоймовірних, але серйозних кіберзагроз	33	15.21
	Зміни у зв'язку з пандемією *COVID*-19 відсутні	4	1.84
	Не знаю / Важко відповісти	10	4.61
Якою має бути роль директора з інформаційної безпеки на підприємстві?	Операційний лідер	48	22.12
	Трансформаційний лідер	28	12.90
	Експерт з кіберстійкості	47	21.66
	Експерт з організації клієнтського досвіду	36	16.59
	Експерт із захисту персональних даних	37	17.05
	Контролер витрат	21	9.68
Яких успіхів досягло ваше підприємство у сфері кібербезпеки за останні три роки?	Підвищення якості управління ризиками (зниження навантаження на співробітників; зниження витрат на забезпечення відповідності вимогам законодавства та стандартів; зниження витрат на управління ризиками)	67	30.88
	Зростання стійкості (скорочення термінів реагування на інциденти та збої; скорочення простоїв та пов'язаних з цим витрат; скорочення числа успішних атак)	61	28.11
	Зростання довіри (підвищення лояльності клієнтів; підвищення індексу споживчої лояльності; суворіше дотримання нормативних вимог; підвищення впевненості керівників)	46	21.20
	Реалізація можливостей бізнесу (прискорення виходу на нові ринки; прискорення запуску нових продуктів; поліпшення клієнтського досвіду; поліпшення досвіду співробітників; більш успішні трансформації)	43	19.82
Які навички повинні бути притаманні фахівцю з кібербезпеки?	Аналітичні здібності	33	15.21
	Креативність	29	13.36
	Робота в команді	21	9.68
	Хмарні рішення	55	25.35
	Управління проєктами	18	8.29
	Робота з даними	19	8.76
	Цифрове проєктування	10	4.61
	Комп'ютерне програмування	8	3.69
	Розробка програмного забезпечення і контроль якості	7	3.23
	Особливі спеціалізації у сфері технологій	5	2.30
	Захист персональних даних	12	5.53
Як зміниться ваш бюджет на кібербезпеку у 2022 р.?	Зменшиться більш ніж на 20 %	4	1.84
	Зменшиться більш ніж на 11–20 %	8	3.69
	Зменшиться більш ніж на 6–10 %	21	9.68
	Знизиться на 5 % або менше	23	10.60
	Підвищиться на 5 % або менше	36	16.59
	Підвищиться на 6–10 %	49	22.58
	Підвищиться більш ніж на 10 %	60	27.65
	Складно спрогнозувати	16	7.37

Джерело: розраховано за даними анкетного опитування 217 респондентів із 45 підприємств України у грудні 2021 р.

Проведене анкетування "Довіра до цифрових технологій" показує, що пандемія й економічний спад сприяють суттєвим змінам: більшість опитаних керівників погоджуються із прискоренням цифровізації. При цьому використовуються нові бізнес-стратегії, про які вони раніше навіть не замислювалися.

Більшість респондентів схиляються до того, щоб розглядати питання кіберуправління з кожним бізнес-рішенням, адже за результатами опитування переважає більш ретельна взаємодія між директором з інформаційної безпеки, генеральним директором та радою директорів. Досвідчені директори з інформаційної безпеки звіряють свої проєкти з концепцією та бізнес-цілями підприємства в цілому, а не тільки з концепцією ІТ-підрозділу.

Таким чином, керівникам з інформаційної безпеки необхідно розвивати нові навички. Учасники опитування ствердили, що хочуть бачити директорів з інформаційної безпеки у ролі трансформаційного лідера або у ролі операційного лідера, водночас це має бути беззаперечний експерт кіберстійкості (див. *табл. 1*). Ці ролі охоплюють різні аспекти, і для їх виконання директори з інформаційної безпеки мають накопичити різнобічний досвід та знання. *Трансформаційний лідер* з інформаційної безпеки керує багатофункціональними робочими групами, підбираючи відповідні стратегії у сфері забезпечення кіберуправління – інформаційної безпеки та захисту персональних даних, забезпечуючи необхідні інвестиції, розробляючи оптимальні плани з урахуванням термінів та масштабів цих програм. *Операційний лідер* – це директор з інформаційної безпеки, який добре розуміється на бізнесі та технологіях і при виникненні загроз здатний забезпечувати стабільну роботу систем із дотриманням належних вимог до безпеки та захист персональних даних на рівні всього підприємства.

Респонденти також визначили успіхи у досягненні цілей кібербезпеки за останні три роки: третина опитаних зауважують підвищення якості управління ризиками, майже третина заявляють про зростання стійкості, п’ята частина керівників говорять про зростання довіри, і майже стільки же звертають увагу на реалізацію можливостей бізнесу. Понад половина опитаних керівників планують збільшити чисельність штатних спеціалістів з кібербезпеки. Навички, наявність яких потрібна новим співробітникам з кіберуправління, – це вміння працювати з технологіями хмарних рішень, аналітичні здібності та креативність. За даними світових досліджень, сьогодні особливо високий попит на фахівців з безпеки хмарних сервісів і аналізу безпеки.

Ймовірність кібератак у 2022 р. вища, ніж будь-коли раніше. Під час війни їх кількість зросла втричі проти минулого року. Можемо спостерігати, що найбільших атак зазнають органи державної влади, медіаресурси, енергетична сфера, сфера логістики. У кіберпросторі росіяни переслідують ті самі цілі, що і їх військові, – завдати якомога більше шкоди інфраструктурі, причому не стільки військовій, скільки цивільній.

Останні роки відзначені сплеском випадків кіберзагроз. За результатами опитування респондентів сформовано карту впливу кіберзагроз на підприємство, що складається з чотирьох сегментів, кожен з яких має певні межі *(рис. 2)*.

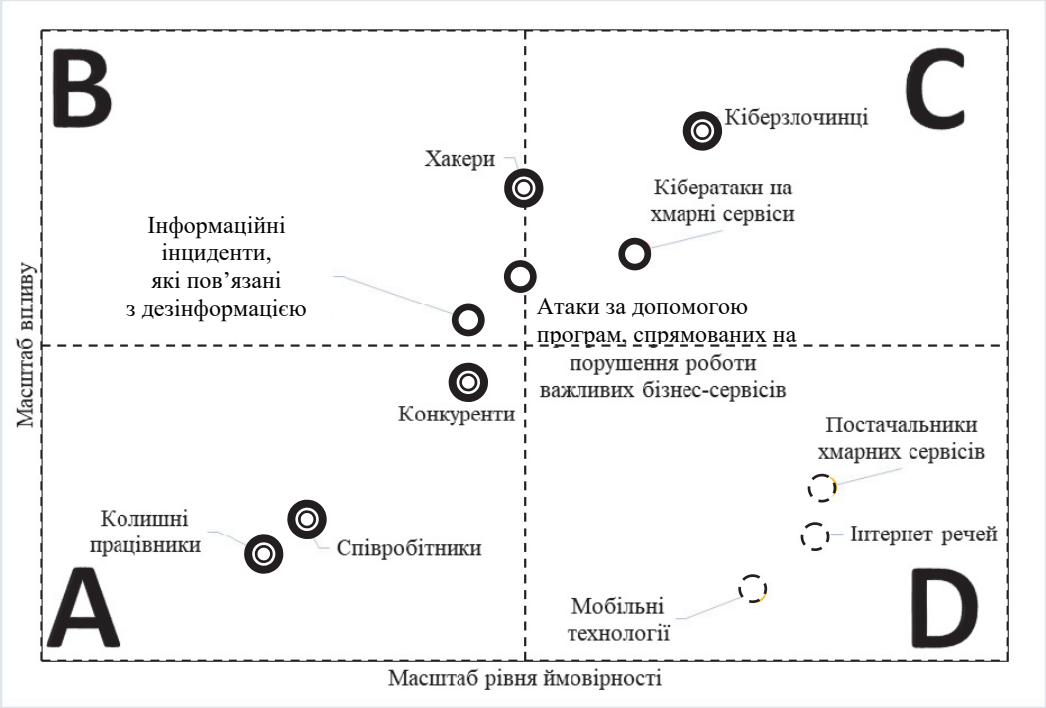

Рис. 2. Карта впливу кіберзагроз на підприємство

Примітка: ◌ – потенційні загрози на 2022 р.; ◎ – потужні й успішні атаки потенційних загроз; ○ – прогноз інцидентів на 2022 р.

Джерело: розраховано авторами за даними анкетного опитування 217 респондентів із 45 підприємств України у грудні 2021 р.

Представлені на карті кіберзагрози можна узагальнити в сегментах залежно від масштабу впливу та масштабу рівня ймовірності. Отже, сегмент *A "Аутсайдер"* – це група, в якій кіберзагрози мають незначну відносну частку. У результаті проведеного опитування визначено ступінь, а також оцінено їхній вплив на підприємство. До сегмента *A* потрапили види кіберзагроз, як-от колишні працівники, конкуренти та співробітники.

Кіберзагрози, що належать до групи *B – "Потенціал"*, мають високі темпи росту: інформаційні інциденти, які пов'язані з дезінформацією. Такі види кіберзагроз, як-от хакери й атаки за допомогою програм, спрямованих на порушення роботи важливих бізнес-сервісів, перебувають на межі від сегмента *B* до сегмента *C "Лідер"* (найпоширеніші загрози). Беззаперечними лідерами кіберзагроз визначено діяльність кіберзлочинців і атаку на хмарні сервіси.

І останній сегмент *D* – *"Генератор"*, це ті, що мають дуже слабкі позиції у списку кіберзагроз. Це зумовлено недостатнім рівнем функціонування. До таких належать постачальники хмарних сервісів, туманних технологій, інтернет речей і мобільні технології.

Таким чином, встановлено, що нова ера кібербезпеки потребує цілком нових підходів до управління підприємством та його ресурсами, зокрема інформаційними. Успіх таких змін значною мірою залежить від того, наскільки гнучко організовані бізнес-процеси на підприємстві, а також як імплементуються нові моделі та методи роботи. Через недоліки в організаційній роботі та невміння управляти змінами підприємства відчувають наслідки кіберризиків, а тому вважаємо за доречне дотримання кібергігієни в умовах *COVID*-реальності *(табл. 2)*.

Таблиця 2

Засоби дотримання кібергігієни в умовах *COVID*-реальності

Напрям/Характеристика	Рекомендації з дотримання кібергігієни
Мережа	
Конфігурація мережі Wi-Fi та налаштування безпеки. Постійно зростає потреба у формуванні безпеки та правильній конфігурації пристроїв, які підключені до мережі *Wi-Fi*, через зростання підключених пристроїв	Зміна паролю на *Wi-Fi*-роутері замість встановленого за замовчуванням; створення паролю для *Wi-Fi* із символів та літер; обмеження кількості пристроїв, які можуть бути підключені до мережі *Wi-Fi*; вибір унікального імені для мережі *Wi-Fi*; увімкнення брандмауера; здійснення регулярного оновлення операційної системи *Wi-Fi*-роутера; налагодження шифрування даних у мережі *Wi-Fi (WPA*2 та *WPA3)*
Ризики під час використання публічних мереж. За безкоштовних та відкритих (публічних) умов використання мереж *Wi-Fi* для хакерів спрощується можливість перебування між точкою доступу *Wi-Fi* та пристроями	Не використовувати відкриті (публічні) мережі *Wi-Fi* для бізнесу, а також обмежити їх використання з метою розваг; перевірка *www*-адрес та роботи *HTTPS*; за можливості застосовувати *VPN*-з'єднання, що захистить від перехоплення даних
Віддалена робота та доступ до мережі	
Аутентифікація, паролі та дані користувача. Хакери посилюють можливості доступу до різноманітних систем, а тому необхідно дотримуватися захисту даних	Регулярно змінювати паролі до особистих облікових записів, а також до програм у робочому середовищі; створювати правильний пароль для *Wi-Fi* із символами та цифрами, а також не менше ніж 10 знаків; використовувати багатофакторну автентифікацію за допомогою програми, *SMS* або дзвінка
Віддалені сесії. До таких сесій належать *VPN* та робота вдома	Під час віддалених сеансів зв'язку з ІТ-інфраструктурою бізнесу доречно застосовувати *VPN* з'єднання; дотримуватися використання багатофакторної автентифікації; без додаткового захисту не користуватися віддаленим підключенням *(TeamViewer, Remote Desktop Protocol)*
Електронна пошта та комунікація	
Безпека. Фішинг електронної пошти. Електронна пошта – найлегший спосіб наживи для зловмисників	Уважно читати вміст електронних листів, а підозрілі файли та листи не відкривати; відкривати листи перевірених та відомих відправників; застосовувати антивірусні програми, за допомогою яких можна перевірити електронну пошту на наявність вірусів
Устаткування для роботи й особистого використання	
Розмежування надмірної експлуатації пристроїв. В умовах онлайн складно розмежувати пристрої для особистого використання та для бізнесу, що провокує кіберризики	Не використовувати робочі пристрої для особистих цілей і навпаки – особисті пристрої для роботи; дотримуватися політики конфіденційності підприємства; встановлювати ліцензійне програмне забезпечення, а також погоджувати це з ІТ-фахівцем; на робочому пристрої не зберігати особистої інформації (документи, файли, результати аналізів чи інші конфіденційні дані); не синхронізувати дані браузера між особистими та робочими пристроями
Мобільні та смартпристрої	
Смартпристрої та дані користувача. Віруси, підозрілі програми, ПЗ без оновлень створюють загрозу безпеці та роблять дані доступними для кіберзлочинців	Посилено використовувати антивірусні програми для захисту; перевіряти та контролювати наданий доступ до програм (наприклад до контактів, камери чи геолокації); уважно аналізувати нетипові запити у соціальних мережах; не встановлювати програми з невідомих джерел; оновлювати програмне забезпечення; використовувати надійні паролі та біометричний захист

Закінчення табл. 2.

Напрям/Характеристика	Рекомендації з дотримання кібергігієни
Мобільні та смартпристрої	
Підключення смартпристроїв до інтернету. Інтернет речей (IoT). Близько 80 % *IoT*-пристроїв не захищено від кібератак	Обирати правильний пристрій, вивчати ліцензію та життєвий цикл пристрою в цілому; використовувати *IoT*-пристрої лише у закритій (приватній) мережі; регулярно оновлювати пристрій та паролі
Робота з даними	
Зберігання даних. Хоча хмара є одним із найефективніших і найсучасніших видів сховищ даних, необхідно переконатися в її кібербезпеці	Доступ до хмари дозволяти лише відомим користувачам та пристроям; не застосовувати відкритої мережі *Wi-Fi* для роботи у хмарі; використовувати багатофакторну автентифікацію для доступу до хмарних ресурсів даних; використовувати шифрування даних як для їх передачі, так і для зберігання
Кіберзнання проти кібершахрайства	
Активність кіберзлочинців розширюється. Нинішня ситуація, спричинена *COVID*-19 і воєнним станом в країні, та віддалена робота створюють сприятливі умови для всіх видів кібершахрайства й атак	Створювати резервні копії; не зберігати конфіденційну інформацію в електронній пошті, а також у незахищеній хмарі або на пристрої, який належним чином не оснащено кіберзахистом; стежити за періодичним оновленням паролів й антивірусних програм; бути уважним до експлуатації електронної пошти; удосконалювати знання з кібербезпеки та кібергігієни

Джерело: сформовано авторами.

Отже, розвиток цифровізації усіх сфер життя сприяє тому, що підприємства та звичайні громадяни дедалі більше потерпатимуть від зростання кіберзлочинності, наприклад, під час придбання товарів чи банківських операцій у мережі Інтернет.

У процесі аналізу стану та тенденцій цифрових технологій як нової ери кібербезпеки сформовано ключові напрями захисту підприємства від кіберзагроз. Щодня набуває актуальності зміна стереотипів у суспільстві стосовно того, що особисті дані чи особа нікому не цікаві, доречно провести навчання фахівців щодо користування захищеними протоколами передачі інформації, застосування захищених інформаційних систем для роботи.

Висновки. Під час вивчення довіри до цифрових технологій як нової ери кібербезпеки здійснено аналіз змін на ринку цифрових технологій у контексті кібербезпеки й обґрунтовано рекомендації з дотримання кібергігієни. Так, за підсумками аналізу встановлено, що для працівників загалом та ІТ-керівників зокрема диджитал-безпека не може залишатися лише стратегією на перспективу, вона має стати запорукою успіху імплементації заходів із переходу на цифрові технології з дотриманням заходів кібергігієни. Також встановлено, що на підприємствах планують збільшити рівень витрат на кібербезпеку у подальшій роботі завдяки дотриманню правил кібергігієни, відповідальному ставленню до політики використання паролів та вчасному оновленню програмного забезпечення, вивченню "вузьких" місць кіберзахисту й інвестуванню в найпростіші способи захисту від кіберзловмисників.

Конфлікт інтересів. Автори заявляють, що вони не мають фінансових чи нефінансових конфліктів інтересів щодо цієї публікації; не мають відносин із державними органами, комерційними або некомерційними організаціями, які могли б бути зацікавлені у поданні цієї точки зору. З огляду на те, що один з авторів працює в установі, яка є видавцем журналу, що може зумовити потенційний конфлікт або підозру в упередженості, остаточне рішення про публікацію цієї статті (включно з вибором рецензентів та редакторів) приймалося тими членами редколегії, які не пов'язані з цією установою.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Дергачова Г. М., Колешня Я. О. Цифрова трансформація бізнесу: сутність, ознаки, вимоги та технології. *Економічний вісник НТУУ "КПІ".* 2020. № 17. С. 280-290.
2. Chapco-Wade C. Digitization, Digitalization, and Digital Transformation: What's the Difference? URL: https://medium.com/@colleenchapco/digitizationdigitalization-and-digital-transformation-whats-thedifference-eff1d002fbdf
3. Bloomberg J. Digitization, Digitalization, And Digital Transformation: Confuse Them At Your Peril. URL: https://www.forbes.com/sites/jasonbloomberg/2018/04/29/digitization-digitalization-and-digital-transformation-confuse-them-at-your-peril/?sh=89ee0042f2c7
4. Круглов В. В. Цифрова трансформація як спосіб побудови смарт-суспільства. URL: https://conf.ztu.edu.ua/wp-content/uploads/2021/01/335.pdf
5. Куйбіда В. С., Карпенко О. В., Наместнік В. В. Цифрове врядування в Україні: базові дефініції понятійно-категорійного апарату. *Вісник НАДУ при Президентові України.* 2018. № 1. С. 5-10.
6. Марущак А. І. Інформаційно-правові аспекти протидії кіберзлочинності. *Інформація і право.* 2018. № 1(24). С. 127-132.
7. Гуцалюк М. В. Окремі аспекти боротьби з організованою кіберзлочинністю. Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук.-практ. конф. (м. Київ, 4 квітня 2019 р.). Київ: Нац. акад. СБУ, 2019. С. 199-201.
8. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва: монографія. Київ: НІСД. 2014. 328 с.
9. Печенюк А. В. Інформаційна безпека України як складова національної безпеки. URL: https://scholar.google.com.ua/citations?view_op=view_citation&hl=uk&user=_Iwh2mAAAAAJ&citation_for_view=_Iwh2mAAAAAJ:M3NEmzRMIkIC
10. Про рішення РНБО України від 14.05.2021 "Про Стратегію кібербезпеки України" від 26.08.2021 № 447/2021: Указ Президента України. URL: https://www.president.gov.ua/documents/4472021-40013
11. Україна 2030Е – країна з розвинутою цифровою економікою. URL: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html

REFERENCES

1. Dergachova, G. M., & Koleshnja, Ja. O. (2020). Cyfrova transformacija biznesu: sutnist', oznaky, vymogy ta tehnologii' [Digital business transformation: essence, features, requirements and technologies]. *Ekonomichnyj visnyk NTUU "KPI" – Economic Bulletin of NTUU "KPI", 17,* 280-290 [in Ukrainian].
2. Chapco-Wade, *C. Digitization, Digitalization, and Digital Transformation: What's the Difference?* https://medium.com/@colleenchapco/digitizationdigitalization-and-digital-transformation-whats-thedifference-eff1d002fbdf [in English].
3. Bloomberg, J. *Digitization, Digitalization, And Digital Transformation: Confuse Them At Your Peril.* https://www.forbes.com/sites/jasonbloomberg/2018/04/29/digitization-digitalization-and-digital-transformation-confuse-them-at-your-peril/?sh=89ee0042f2c7 [in English].
4. Kruglov, V. V. *Cyfrova transformacija jak sposib pobudovy smart-suspil'stva [Digital transformation as a way to build a smart society].* https://conf.ztu.edu.ua/wp-content/uploads/2021/01/335.pdf [in Ukrainian].
5. Kujbida, V. S., Karpenko, O. V., & Namestnik, V. V. (2018). Cyfrove vrjaduvannja v Ukrai'ni: bazovi definicii' ponjatijno-kategorijnogo aparatu [Digital governance in Ukraine: basic definitions of the conceptual and categorical apparatus]. *Visnyk NADU pry Prezydentovi Ukrai'ny – NAPA Bulletin under the President of Ukraine, 1,* 5-10 [in Ukrainian].

6. Marushhak, A. I. (2018). Informacijno-pravovi aspekty protydii' kiberzlochynnosti [Information and legal aspects of combating cybercrime]. *Informacija i pravo – Information and law, 1*(24), 127-132 [in Ukrainian].
7. Gucaljuk, M. V. (2019). Okremi aspekty borot'by z organizovanoju kiberzlochynnistju. Aktual'ni problemy upravlinnja informacijnoju bezpekoju derzhavy [Some aspects of the fight against organized cybercrime. Current issues of information security management of the state]. *Zbirnyk tez naukovo-praktychnoi' konferencii' – Collection of abstracts of the scientific-practical conference*. (pp. 199-201). Kyi'v: Nacional'na akademija SBU [in Ukrainian].
8. Dubov, D. V. (2014). *Kiberprostir jak novyj vymir geopolitychnogo supernyctva [Cyberspace as a new dimension of geopolitical rivalry]*. Kyi'v: NISD [in Ukrainian].
9. Pechenjuk, A. V. *Informacijna bezpeka Ukrai'ny jak skladova nacional'noi' bezpeky [Information security of Ukraine as a component of national security]*. https://scholar.google.com.ua/citations?view_op=view_citation&hl=uk&user=_Iwh2mAAAAAJ&citation_for_view=_Iwh2mAAAAAJ:M3NEmzRMIkIC [in Ukrainian].
10. *Pro rishennja RNBO Ukrai'ny vid 14.05.2021 "Pro Strategiju kiberbezpeky Ukrai'ny" vid 26.08.2021 № 447/2021: Ukaz Prezydenta Ukrai'ny [On the decision of the National Security and Defense Council of Ukraine dated 14.05.2021 "On the Cyber Security Strategy of Ukraine" dated 26.08.2021 № 447/2021: Decree of the President of Ukraine]*. https://www.president.gov.ua/documents/4472021-40013 [in Ukrainian].
11. *Ukrai'na 2030E – krai'na z rozvynutoju cyfrovoju ekonomikoju [Ukraine 2030E is a country with a developed digital economy]*. https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html [in Ukrainian].

Надійшла до редакції 21.02.2022.
Прийнято до друку 02.05.2022.
Публікація онлайн 23.09.2022.