

ДОСЛІДЖЕННЯ ЗМІН В ЕКОНОМІЧНІЙ, СОЦІАЛЬНІЙ ТА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ¹

EXPLORING CHANGES IN ECONOMIC, SOCIAL AND INFORMATION SECURITY IN THE CONTEXT OF DIGITAL TRANSFORMATION

Діджиталізація є основою розвитку багатьох сфер на сьогоднішній день. В тому числі цифровізації зазнають економіка та соціальна сфера, багато інформації переноситься в цифровий формат, що створює нові виклики та загрози як для пересічного громадянина, так і для великих промислових підприємств. Метою статті є аналіз даних за останні 5 років щодо кіберзагроз економічній, соціальній та інформаційній безпеці із використанням статистики від провідних IT-фірм, таких як IBM та ECS, а також статистичних порталів Statista та OECD Data. Статистика показує що кіберзлочинці урізноманітнюють свою тактику щороку, а збитки від кіберзлочинності в усьому світі за 2023 рік оцінюються у 8 мільярдів доларів США, прогнозована сума збитків за 2024 рік становить 9,5 мільярдів доларів, а на кінець 2025 року ця сума може досягти 10,5 мільярдів доларів США. Розвинені країни Європейського Союзу мають значні видатки на соціальний захист населення, що показує пріоритетність даного напрямку та надає додаткові можливості населенню. Отримані результати показують що діджиталізація, окрім явних позитивних ефектів, зокрема підвищення соціальної стабільності, доступності ресурсів для слабо захищених верств населення, спрощення механізмів урядування, з кожним роком завдає все більше і більше збитків в цілому економіці та приватним громадянам зокрема. Отримання доступу до персональних та конфіденційних даних зловмисниками є розповсюдженим явищем, особливо у розвинених країнах, та країнах зі слабкою цифровою грамотністю населення. Аналіз даних тенденцій має бути регулярним та різнобічним для своєчасного виявлення загроз та реакції на них відповідних державних служб та приватних спеціалістів.

Ключові слова: діджиталізація, економічна безпека, соціальна безпека, інформаційна безпека, кіберзагроза, статистика, аналіз даних.

Digitalization is the basis for the development of many areas today. The economy and the social sphere are also undergoing digitalization, and a lot of information is being transferred to digital format, which creates new challenges and threats for both ordinary citizens and large industrial enterprises. The purpose of the article is to analyze the data for the last 5 years on cyber threats to economic, social and information security using statistics from leading IT firms such as IBM and ECS, as well as statistical portals Statista and OECD Data. The statistics show that cybercriminals diversify their tactics every year and the losses from cybercrime worldwide in 2023 were estimated at USD 8 billion, the projected number of losses for 2024 is USD 9.5 billion, and by 2025 the annual amount of losses could reach USD 10.5 billion. In the developed countries of the European Union, social spending is quite high, which means that the development of this area is a priority and provides the population with additional opportunities. The results of the research show that digitalization, in addition to its obvious positive effects, such as increased social stability, access to resources for vulnerable groups, and simplification of governance mechanisms, is causing more and more damage to economics in general and private citizens in particular every year. Gaining access to personal and confidential data by malicious actors is a widespread phenomenon, especially in developed countries and countries with low digital literacy. The analysis of these trends should be regular and comprehensive to ensure timely detection of threats and responses by relevant public services and private specialists.

Key words: digitalization, economic security, social security, information security, cyber threat, statistics, data analysis.

УДК 004.056:316.4:338.2

DOI: <https://doi.org/10.32782/dees.17-48>

Островський О.О.

аспірант,

Сумський державний університет

Кубатко О.В.²

д.е.н., професор,

професор кафедри економіки,

підприємництва

та бізнес-адміністрування,

Сумський державний університет

Гриценко К.Г.

к.т.н., доцент кафедри економічної

кібернетики,

Сумський державний університет

Ostrovsky Oleksandr

Sumy State University

Kubatko Olexandr

Sumy State University

Hrytsenko Kostyantyn

Sumy State University

Постановка проблеми. Діджиталізація є невід'ємною частиною усіх процесів та перетворень, які відбуваються майже щоденно у сучасному світі, її стрімкі темпи несуть за собою відчутні переваги для багатьох сфер, в яких функціонує суспільство. Але з іншого боку цифровізація приносить і значний обсяг нових проблем та викликів, з якими людство раніше не стикалось через відсутність технологічних передумов. Зберігання великих обсягів конфіденційної інформації громадян у мережі та хмарних сервісах, оцифровування великих обсягів даних, перенесення персональних даних громадян в цифровий формат – ці процеси

тягнуть за собою потенційні ризики та дають підґрунтя для вчинення злочинних дій у цифровій сфері, так званих кіберзлочинів. Дослідження змін в економічній, соціальній та інформаційній безпеці є важливим питанням на сьогодні для повного та чіткого розуміння проблем та викликів, які ставить перед суспільством процес діджиталізації.

Аналіз останніх досліджень і публікацій. Питаннями дослідження впливу кіберзагроз на різні сфери життя населення займаються як вітчизняні, так і зарубіжні науковці, а також всесвітньо відомі організації, які мають значну вагу у питаннях діджиталізації та інформаційних технологій.

¹ Робота виконана в рамках НДР «Цифрові трансформації для забезпечення цивільного захисту та повоєнного відновлення економіки в умовах екологічних і соціальних викликів» та Jean Monnet Module «Disruptive technologies for sustainable development in conditions of Industries 4.0 and 5.0: the EU Experience», (101083435-DTSDI-ERASMUS-JMO-2022-HEI-TCH-RSCH)

² ORCID: <https://orcid.org/0000-0001-6396-5772>

Зокрема, IBM Security – підрозділ компанії IBM, який спеціалізується на послугах з кібербезпеки для підприємств, щороку розраховує індекс загроз (X-Force Threat Intelligence Index) [1], який розподіляє галузі за частками кібератак на них серед усіх кібератак у світі. Компанія Microsoft проводить активні дослідження напрямків та цілей кібератак, досліджує кіберзагрози у своїх спеціалізованих підрозділах Cyber Defense Operations Center та Microsoft Threat Intelligence. Компанія надає інструменти такі як Azure Security Center або Microsoft Defender, а також запроваджує освітні програми з безпечного користування Інтернетом для різних верств населення, надає регулярні звіти та співпрацює з державними установами країн для підвищення загального рівня кібербезпеки [2]. Компанія Apple регулярно публікує звіти про виявлені та потенційні загрози, оновлення безпеки та тренди у кіберзахисті для інформування користувачів, а також реалізовує програму винагород для фахівців із дослідження безпеки, спонукаючи до пошуку вразливостей для вдосконалення своїх продуктів [3]. Серед зарубіжних науковців, що досліджували вплив діджиталізації на економічну, соціальну та інформаційну безпеку, можна виділити: T. Gibbs [4], Z. Nyikes, T. A. Kovács, V. S. Honfi, Z. Illési [5], Almeida F., Duarte Santos J., Augusto Monteiro J. [6], Rymarczyk J. [7], B. Lee-Archer [8], A. Hosny, A. Sollaci [9]. Серед вітчизняних вчених, що досліджували дане питання, можна виділити: О. Кужур, Т. Васильєва, О. Кузьменко, В. Койбічук, Р. Brožek [10], І. Шахина, О. Подзигун, А. Петрова, Г. Гордійчук [11], Я. Самусевич, В. Новіков, А. Артюхов, Т. Васильєва [12], С. Бондаренко, О. Макеева, О. Усаченко, В. Веклич, Т. Аріфходжаєва [13], В. Онищенко, С. Єгоричева, О. Маслій, Н. Юрків [14].

Постановка завдання. Метою статті є дослідження змін в економічній, соціальній та інформаційній безпеці в умовах цифрової трансформації за останні 5 років на основі статистичних даних, а також виявлення ключових безпекових викликів стабільному розвитку суспільства, які створює цифровізація.

Виклад основного матеріалу дослідження. Протягом останніх років науковці відмічають той факт, що цифрова трансформація, незважаючи на численні переваги, стає підґрунтям для виникнення значної кількості загроз, зокрема кіберзлочинів. Для кращого розуміння об'єкту дослідження необхідно навести визначення таких понять як «інформаційна безпека», «соціальна безпека», «економічна безпека», «кіберзлочин».

Економічна безпека на національному рівні означає захищеність, стійкість та стабільність економіки від внутрішніх і зовнішніх загроз, а також здатність країни досягати цілей розвитку своєї економіки. Економічна безпека часто прямо пов'язана

із національною безпекою, адже включає в себе питання торговельного балансу, впливу іноземних інвестицій на національні ринки та державно-приватного партнерства [15].

Соціальна безпека визначає програму соціального захисту, встановлену законодавством, або будь-яку іншу державну обов'язкову програму, яка забезпечує людям певний рівень доходу та доступ до основних благ і послуг, які є необхідними для нормальної життєдіяльності в разі виникнення непередбачуваних обставин, таких як: старість, інвалідність, безробіття, втрата годувальника, недієздатність [16].

Під інформаційною безпекою зазвичай мається на увазі практика захисту інформації шляхом зменшення інформаційних ризиків. Вона має на меті захист інформаційних систем та власне інформації, яка оброблюється, зберігається та передається такими системами, від розкриття, несанкціонованого доступу, модифікації або знищення, витоків, неналежного використання [17].

Поняття кіберзлочину визначається п. 8 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII як «суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України» [18].

Зазвичай кіберзлочину передуює кібератака, яка є наслідком наявності вразливих місць у кіберзахисті, неуважності користувача, або випадкових помилок. Кібератаки можуть бути спрямовані на широке коло жертв: від окремих користувачів мережі до підприємств, установ та урядів країн. Найпоширенішими типами кібератак є: шкідливе програмне забезпечення, тунелювання DNS, відмова в обслуговуванні (DoS), фішинг, спуфінг, атаки на основі Інтернету речей та ідентифікації, ін'єкції коду, атаки на ланцюги поставок, внутрішні загрози.

Статистичні дані показують невтішну тенденцію: кіберзлочинці щороку диверсифікують свою тактику і вже не залишилось такого сектору людської життєдіяльності, який би не був ціллю для кібератак. Збитки від кіберзлочинів по всьому світу у 2023 році оцінювались у 8 трлн дол США, прогноною сумою збитків за 2024 рік є 9,5 трлн дол США, а до 2025 року річна сума збитків може сягнути 10,5 трлн дол США, що є більш ніж втричі більшим значенням за дані 2015 року, коли загальна річна сума збитків була на рівні 3 трлн дол США [19].

Згідно даних компанії IBM Security (таблиця 1) протягом 2021–2023 рр. найбільш атакованою була галузь виробництва, яка змістила з першого місця галузь фінансів та страхування,

Таблиця 1

Розподіл часток сумарної кількості кібератак за галузями протягом 2019–2023 рр.

Галузь	Рік				
	2019	2020	2021	2022	2023
Виробництво	8,0%	17,7%	23,2%	24,8%	25,7%
Фінанси та страхування	17,0%	23,0%	22,4%	18,9%	18,2%
Професійні та побутові послуги	10,0%	8,7%	12,7%	14,6%	15,4%
Енергетика	6,0%	11,1%	8,2%	10,7%	11,1%
Роздрібна та оптова торгівля	16,0%	10,2%	7,3%	8,7%	10,7%
Освіта	8,0%	4,0%	2,8%	7,3%	2,8%
Охорона здоров'я	3,0%	6,6%	5,1%	5,8%	6,3%
Державне управління	8,0%	7,9%	2,8%	4,8%	4,3%
Транспорт	13,0%	5,1%	4,0%	3,9%	4,3%
Медіа та телекомунікації	10,0%	5,7%	2,5%	0,5%	1,2%

Джерело: розроблено автором на основі даних IBM [1]

що лідирувала за кількістю кібератак протягом 2019–2020 рр. Незважаючи на щорічне збільшення витрат у сфері кібербезпеки, близько 51% компаній-виробників зазнали відчутних кібератак на свою хмарну інфраструктуру протягом 2022 року.

У таблиці 2 наведена інформація про 5 наймасштабніших кібератак у сфері виробництва за останні 5 років. Аналізуючи дані, наведені у таблиці, можна зробити висновок, що атаки на сферу виробництва є дійсно масштабними та серйозними, і призводять не тільки до фінансових втрат компаній, а і до збоїв у їхніх ланцюгах постачання, що є відчутним ударом по світовій економіці.

Переходячи до питання зв'язку діджиталізації та інформаційної безпеки необхідно визначити масштаб загрози від використання мережі для населення.

Відповідно до графіку (рисунок 1) за 2022 рік найбільш атакованими були громадяни Індії, США та Австралії, а глобально, хоча б одну кібератаку протягом 2022 року зазнали 39% усіх користувачів Інтернету. Дана статистика є досить показовою,

адже причини кібератак на розвинені країни є зрозумілими – кіберзлочинці атакують як окремих громадян, так і компанії, шукаючи фінансову вигоду, висока концентрація цінних цілей робить такі країни як: США, Австралія, Нова Зеландія, Франція, Великобританія, Німеччина, Японія бажаними цілями для зловмисників. Але першою за кількістю кібератак є Індія, яка відноситься до країн, що розвиваються, і причиною цього є цифровий розрив у країні.

Розглядаючи зв'язок діджиталізації та соціальної безпеки треба згадати той факт, що багато країн завдяки Цілям сталого розвитку поставили перед собою амбітні завдання щодо покращення систем соціального захисту та охорони здоров'я. Проте базові статистично-облікові дані, такі як: записи про народження і смерть, або домогосподарства, з доходами, що нижчі за національну межу бідності, відсутні, або не мають зв'язку між собою. Політики та керівники служб не мають достатньо надійної інформації аби приймати обґрунтовані рішення про те, куди треба направити ресурси, або які заходи є ефективними.

Таблиця 2

Наслідки 5 наймасштабніших кібератак у сфері виробничої промисловості за 2019–2024 рр.

Рік	Назва компанії, сфера	Наслідки кібератаки
2024	CDK Global, програмне забезпечення	Виведено з ладу тисячі автосалонів, що покладаються на платформу компанії, злочинцям виплачено викуп у розмірі ймовірно 22 млн дол США
2023	Brunswick Corporation, суднобудування	Зупинка роботи на декількох заводах, збитки на суму щонайменше 85 млн дол США
2022	Toyota Motor, автомобілебудування	Зупинка 14 внутрішніх виробничих ліній, втрата 375 млн дол США
2021	JBS, харчова промисловість	Збій у глобальних операціях компанії, виробництві та поставках м'яса у кількох країнах на тиждень, вимога викупу у розмірі 11 млн дол США за розшифровку даних та запобігання витоку конфіденційної інформації
2020	Renault-Nissan, автомобілебудування	Тимчасова зупинка виробництва на 5 заводах, збитки у розмірі 4 млрд дол США

Джерело: розроблено автором на основі даних ECS [20]

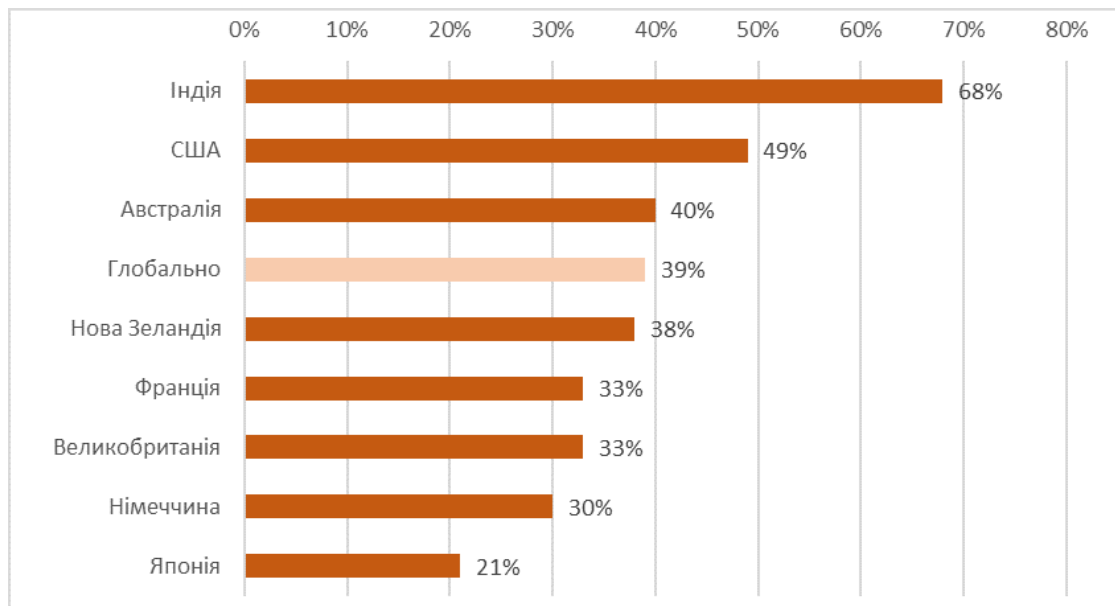


Рис. 1. Відсоток інтернет-користувачів за країнами, які хоча б раз постраждали від кібератаки протягом 2022 року

Джерело: складено автором на основі даних статистичного сайту Statista [21]

Виходячи з даних таблиці 3, можна зробити висновок, що соціальній безпеці у країнах Євросоюзу приділяється значна увага, наприклад, у Франції в 2022 р. на фінансування соціального захисту було виділено 31,6 % ВВП, в Італії – 30,1 %, в Австрії – 29,4 %. Однією з визначальних рис сфери соціального захисту є одночасно досить високий попит на її блага і значна трудомісткість їх створення, що є причиною високих державних витрат на соціальну безпеку, а діджиталізація даної сфери має надати можливості для реальних змін у способах надання послуг. На сьогоднішній день

у країнах Європи реалізована достатньо велика кількість проєктів із цифровізації сфери соціального захисту, наприклад, у охороні здоров'я, освіті, наданні фінансової допомоги та персональної фізичної підтримки [23]. Цифровізація систем соціального захисту може зробити їх безпечнішими та зв'язаними одна з одною, покращить доступ, зменшить витрати, підвищить якість та персоналізує послуги. Бідні сім'ї зможуть отримувати підтримку від держави, особливо під час криз, або для створення та запуску схем медичного страхування чи пенсійних виплат [24].

Таблиця 3

Країни Євросоюзу з найвищими державними соціальними видатками протягом 2015–2022 рр., у % від ВВП

Країна	Рік							
	2022	2021	2020	2019	2018	2017	2016	2015
Франція	31,63	32,66	34,88	30,74	30,99	31,45	31,92	31,78
Італія	30,06	30,73	32,63	27,73	27,52	27,65	27,93	28,32
Австрія	29,36	31,06	31,11	27,71	27,56	27,83	28,20	28,26
Фінляндія	29,02	30,34	31,00	29,42	29,35	29,57	30,44	30,53
Бельгія	28,96	29,70	32,28	28,22	28,36	28,27	28,43	29,05
Іспанія	28,09	29,54	31,18	24,65	24,03	23,93	24,25	24,71
Німеччина	26,72	27,64	27,94	25,59	25,30	25,24	25,28	25,07
Данія	26,16	28,27	29,35	28,44	28,53	28,98	29,43	29,98
Португалія	24,64	24,80	25,11	22,34	22,46	22,73	23,46	23,92
Греція	24,11	26,10	27,86	25,08	25,02	25,19	26,04	25,72

Джерело: розроблено автором на основі даних OECD Data [22]

Висновки з проведеного дослідження.

Підсумовуючи наведені статистичні дані щодо впливу діджиталізації на економічну, соціальну та інформаційну безпеку, можна побачити як цифрова трансформація безпосередньо та суттєво впливає на дані сфери життєдіяльності громадян по всьому світу, і, нажаль, не найкращим чином. З одного боку переваги запровадження автоматизованих систем у сфері виробництва, фінансів, урядування, тощо, є значними, але з іншого боку значно зростає кількість кіберзагроз та кібератак, які спрямовані на отримання персональних даних користувачів, або конфіденційних даних підприємств. Створюється нове поле для злочинності, кількість кіберзлочинів зростає щорічно, а втрати від них інколи сягають сотень мільйонів доларів США. Проте, якщо вміло протидіяти злочинцям та чітко вибудовувати систему захисту інформації в Інтернеті, то плюси використання інформаційних технологій переважать мінуси, як, наприклад, це спостерігається у соціальній сфері різних країн, де значно зростає доступ до соціальної взаємодії як між громадянами, так і між владою та населенням. Важливо продовжувати дослідження даної проблеми, аналізувати статистичні дані, виявляти тенденції, для того щоб знаходити чіткий баланс між перевагами та недоліками масової діджиталізації в епоху цифрового розвитку.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. IBM Security X-Force threat intelligence index 2024. IBM. URL: <https://www.ibm.com/reports/threat-intelligence>
2. Cybersecurity awareness – education and resources. Microsoft. URL: <https://www.microsoft.com/en-us/security/business/cybersecurity-awareness>
3. Apple security research. Apple. URL: <https://security.apple.com/>
4. Gibbs T. Seeking economic cyber security: a Middle Eastern example. *Journal of money laundering control*. 2020. Vol. 23. No. 2. P. 493–507. DOI: <https://doi.org/10.1108/jmlc-09-2019-0076>
5. Nyikes Z. et al. Digital competence and security awareness from the perspective of sustainability. *Security-Related advanced technologies in critical infrastructure protection*. Dordrecht, 2022. P. 139–150. DOI: https://doi.org/10.1007/978-94-024-2174-3_12
6. Almeida F., Duarte Santos J., Augusto Monteiro J. The challenges and opportunities in the digitalization of companies in a post-covid-19 world. *IEEE engineering management review*. 2020. Vol. 48. No. 3. P. 97–103. DOI: <https://doi.org/10.1109/emr.2020.3013206>
7. Rymarczyk J. Technologies, opportunities and challenges of the industrial revolution 4.0: theoretical considerations. *Entrepreneurial business and economics review*. 2020. Vol. 8. No. 1. P. 185–198. DOI: <https://doi.org/10.15678/eber.2020.080110>
8. Lee-Archer B. Effects of digitalization on the human centrality of social security administration and services. *International Labour Organization*. URL: <https://www.ilo.org/static/english/intserv/working-papers/wp087/index.html>
9. Hosny A., Sollaci A. Digitalization and social protection: macro and micro lessons for Vietnam. *IMF working papers*. 2022. Vol. 2022. No. 185. P. 1. DOI: <https://doi.org/10.5089/9798400220029.001>
10. Kuzior A. et al. Global digital convergence: impact of cybersecurity, business transparency, economic transformation, and AML efficiency. *Journal of open innovation: technology, market, and complexity*. 2022. Vol. 8. No. 4. P. 195. DOI: <https://doi.org/10.3390/joitmc8040195>
11. Shakhina I. et al. Digitalization as a prospective direction of the contemporary education system. *Modern information technologies and innovation methodologies of education in professional training methodology theory experience problems*. 2022. P. 65–77. DOI: <https://doi.org/10.31652/2412-1142-2022-63-65-77>
12. Samusevych Y. V. et al. Convergence trends in the "economy – education – digitalization – national security". *Науковий вісник НГУ*. 2021. No. 6. P. 177–183. DOI: <https://doi.org/10.33271/nvngu/2021-6/177>
13. Bondarenko S. et al. The Legal Mechanisms for Information Security in the context of Digitalization. *Journal of information technology management*. 2022. Vol. 14. P. 25–58. DOI: <https://doi.org/10.22059/jitm.2022.88868> (date of access: 29.10.2024).
14. Onyshchenko V. et al. Impact of Innovation and Digital Technologies on the Financial Security of the State. *Proceedings of the 3rd International Conference on Building Innovations*. 2021. P. 749–759. DOI: https://doi.org/10.1007/978-3-030-85043-2_69
15. Mollenkamp D. T. Economic security: meaning, history in the US, FAQs. Investopedia. URL: <https://www.investopedia.com/economic-security-5213404>
16. Social security: a fundamental human right. International social security association. URL: <https://www.issa.int/about/socialsecurity>
17. What is information security?. GeeksforGeeks. URL: <https://www.geeksforgeeks.org/what-is-information-security/>
18. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII : станом на 1 січ. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
19. Morgan S. Cybercrime to cost the world \$9.5 trillion USD annually in 2024. *Cybercrime Magazine*. URL: <https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024>
20. Robert P. Manufacturing cybersecurity statistics: recent cyber security attacks, risks & threats to manufacturing industry. Expert Computer Solutions. URL: <https://www.ecsoffice.com/manufacturing-cybersecurity-statistics/>
21. Petrosyan A. Cybercrime rate by country 2022. Statista. URL: <https://www.statista.com/statistics/194133/cybercrime-rate-in-selected-countries/>
22. Social protection – Social spending. OECD. URL: <https://www.oecd.org/en/data/indicators/social-spending.html>
23. Fedirko N. Digital social protection in Ukraine: prerequisites and strategic challenges. *Social and labour relations: theory and practice*. 2022. Vol. 12.

No. 1. P. 1–13. DOI: [https://doi.org/10.21511/slrrp.12\(1\).2022.01](https://doi.org/10.21511/slrrp.12(1).2022.01)

24. Questions and answers on digitalisation in social security coordination. European Commission. URL: https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_4264

REFERENCES:

1. IBM Security X-Force threat intelligence index 2024. IBM. Available at: <https://www.ibm.com/reports/threat-intelligence>
2. Cybersecurity awareness – education and resources. Microsoft. Available at: <https://www.microsoft.com/en-us/security/business/cybersecurity-awareness>
3. Apple security research. Apple. Available at: <https://security.apple.com/>
4. Gibbs T. (2020) Seeking economic cyber security: a Middle Eastern example. *Journal of money laundering control*, vol. 23, no. 2, pp. 493–507. DOI: <https://doi.org/10.1108/jmlc-09-2019-0076>
5. Nyikes Z. et al. Digital competence and security awareness from the perspective of sustainability. *Security-Related advanced technologies in critical infrastructure protection*. Dordrecht, 2022. P. 139–150. DOI: https://doi.org/10.1007/978-94-024-2174-3_12
6. Almeida F., Duarte Santos J., Augusto Monteiro J. (2020) The challenges and opportunities in the digitalization of companies in a post-covid-19 world. *IEEE engineering management review*, vol. 48, no. 3, pp. 97–103. DOI: <https://doi.org/10.1109/emr.2020.3013206>
7. Rymarczyk J. (2020) Technologies, opportunities and challenges of the industrial revolution 4.0: theoretical considerations. *Entrepreneurial business and economics review*, vol. 8, no. 1, pp. 185–198. DOI: <https://doi.org/10.15678/eber.2020.080110>
8. Lee-Archer B. Effects of digitalization on the human centrality of social security administration and services. *International Labour Organization*. Available at: <https://www.ilo.org/static/english/intserv/working-papers/wp087/index.html>
9. Hosny A., Sollaci A. (2022) Digitalization and social protection: macro and micro lessons for Vietnam. *IMF working papers*, no. 185, p. 1. DOI: <https://doi.org/10.5089/9798400220029.001>
10. Kuzior A. et al. (2022) Global digital convergence: impact of cybersecurity, business transparency, economic transformation, and AML efficiency. *Journal of open innovation: technology, market, and complexity*, vol. 8, no. 4, pp. 195. DOI: <https://doi.org/10.3390/joitmc8040195>
11. Shakhina I. et al. (2022) Digitalization as a prospective direction of the contemporary education system. *Modern information technologies and innovation methodologies of education in professional training methodology theory experience problems*, pp. 65–77. DOI: <https://doi.org/10.31652/2412-1142-2022-63-65-77>
12. Samusevych Y. V. et al. (2021) Convergence trends in the "economy – education – digitalization – national security". *Naukovyi visnyk NHU*, no. 6, pp. 177–183. DOI: <https://doi.org/10.33271/nvngu/2021-6/177>
13. Bondarenko S. et al. (2022) The Legal Mechanisms for Information Security in the context of Digitalization. *Journal of information technology management*, vol. 14, pp. 25–58. DOI: <https://doi.org/10.22059/jitm.2022.88868> (date of access: 29.10.2024).
14. Onyshchenko V. et al. (2021) Impact of Innovation and Digital Technologies on the Financial Security of the State. Proceedings of the 3rd International Conference on Building Innovations, pp. 749–759. DOI: https://doi.org/10.1007/978-3-030-85043-2_69
15. Mollenkamp D. T. Economic security: meaning, history in the US, FAQs. Investopedia. Available at: <https://www.investopedia.com/economic-security-5213404>
16. Social security: a fundamental human right. International social security association. Available at: <https://www.issa.int/about/socialsecurity>
17. What is information security?. GeeksforGeeks. Available at: <https://www.geeksforgeeks.org/what-is-information-security/>
18. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [On the basic principles of ensuring cybersecurity in Ukraine]. Zakon Ukrainy vid 05.10.2017 r. № 2163-VIII : stanom na 1 sich. 2024 r. Available at: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
19. Morgan S. Cybercrime to cost the world \$9.5 trillion USD annually in 2024. Cybercrime Magazine. Available at: <https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024>
20. Robert P. Manufacturing cybersecurity statistics: recent cyber security attacks, risks & threats to manufacturing industry. Expert Computer Solutions. Available at: <https://www.ecsoffice.com/manufacturing-cybersecurity-statistics/>
21. Petrosyan A. Cybercrime rate by country 2022. Statista. Available at: <https://www.statista.com/statistics/194133/cybercrime-rate-in-selected-countries/>
22. Social protection – Social spending. OECD. Available at: <https://www.oecd.org/en/data/indicators/social-spending.html>
23. Fedirko N. (2022) Digital social protection in Ukraine: prerequisites and strategic challenges. *Social and labour relations: theory and practice*, vol. 12, no. 1, pp. 1–13. DOI: [https://doi.org/10.21511/slrrp.12\(1\).2022.01](https://doi.org/10.21511/slrrp.12(1).2022.01)
24. Questions and answers on digitalisation in social security coordination. European Commission. Available at: https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_4264