ІНФОРМАЦІЙНА СКЛАДОВА ЕКОНОМІЧНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ
INFORMATION COMPONENT OF ECONOMIC SECURITY OF THE ORGANIZATION

УДК: 658.5:338.2
DOI: https://doi.org/10.32782/dees.3-14

Кір'ян О.І.[1]
к.е.н., доцент,
доцент кафедри економіки
та менеджменту,
Українська інженерно-педагогічна
академія
Кононенко Я.В.[2]
к.е.н.,
доцент кафедри економіки
та менеджменту,
Харківський національний університет
імені В.Н. Каразіна
Торяник Д.О.[3]
аспірант кафедри економіки
та менеджменту,
Українська інженерно-педагогічна
академія

Kirian Olena
Ukrainian Engineering Pedagogics
Academy
Kononenko Yana
V.N. Karazin Kharkiv National University
Torianyk Denys
Ukrainian Engineering Pedagogics
Academy

Глобалізаційні процеси в економіці, стрімкі зміни зовнішнього середовища, розвиток інформаційних технологій змінили сучасні вимоги до діяльності кожного суб'єкта господарювання, вимагаючи, з одного боку, впровадження в діяльність цифровізації, з іншого – суттєвого оновлення та посилення інформаційної безпеки як складової економічної безпеки. Забезпечення економічної безпеки в нових умовах є ключовим питанням сучасної організації, чинником утримання іміджу та прибутковості. В статті висвітлено основні законодавчі вимоги до роботи організації з інформацією, їх досить проблемні для практичної реалізації протиріччя. Розкрито вплив людського чинника на можливе формування небезпек з визначенням напрямів їх можливої нейтралізації. Зроблено наголос на необхідності постійного прогнозування доцільності впровадження диджиталізації та новітніх інформаційних технологій в діяльність організації. Приділено увагу кібербезпеці як складовій економічної безпеки організації.
Ключові слова: *цифровізація, диджиталізація, цифрова економіка, бізнес-середовище, систематизація інформації, економічна безпека, інформаційна небезпека, кібербезпека.*

The purpose of the work is to determine the issues of economic security in view of modern aspects of the organization's activities: the need to strengthen economic security and the simultaneous implementation of digitization and digitalization, new information systems. Globalization processes in the economy, rapid changes in the external environment, and the development of information technologies have changed the modern requirements for the activities of each business entity. The development of society and technology requires the introduction of digitization and digitization as modern elements of the organization's average activity. However, this requires significant updating and strengthening of information security as a component of economic security. Ensuring economic security in new conditions is a key issue of modern organization. It is a factor in image maintenance and profitability. This determines the relevance of the topic of the work. The work uses methods of observation, synthesis, and decomposition. The article highlights the main requirements of domestic legislation for the organization's work with information. It is shown that they are rather problematic for practical implementation of contradictions – transparency, openness and security of information at the same time. The article shows to a greater extent the influence of the human factor on the possible creation of dangerous situations in the information space. Emphasis is placed on the need for constant forecasting of the expediency of implementing digitization and the latest information technologies, new equipment in the organization's activities. Attention is paid to cyber security as a component of economic security of the organization. The article offers a list of directions for possible neutralization of informational hazards. Among them, special attention is paid to the development of personnel as the main factor of conscious activity in the information space. In addition, emphasis was placed on the need to form and constantly update the information and economic security system; adding a cyber-security system to it. Attention is paid to the need to control activities, personnel, and information systems. The question of the need to implement a system of naming and saving electronic documentation was raised. Each risk to economic security discussed in the article has a unique prevention and neutralization solution for each organization. In the same way, each proposed direction of optimization of information security will allow management to focus on comprehensive problem solving when forming an updated management system of the organization. Each element from the list can be a topic for further research.
Key words: *digitization, digitalization, digital economy, business environment, systematization of information, economic security, information danger, cyber security.*

Постановка проблеми. Глобалізація економічного простору, з одного боку, та поступове безперечне домінування цифровізації, з іншого, змушує сучасні організації по новому підходити до процесів забезпечення економічної безпеки їх діяльності. Стрімкий розвиток технологій, потреба в їх активному впровадженні для убезпечення необхідного рівня відповідності сучасному світу та конкурентоспроможності, привабливості для клієнтів в тому числі наявною сучасною системою управління та не завжди підготовлений до цього персонал та інші системи управління можуть створювати значну загрозу економічній безпеці організації. Тому в сучасних процесах управління економічною безпекою підприємства інформаційна складова – її врахування, убезпечення в процесі розвитку стає для багатьох складною проблемою, що обумовлює важливість наукового дослідження цього питання.

Аналіз сучасних досліджень і публікацій. Сучасна світова економіка перейшла на новий рівень. З повним правом можна стверджувати, що настала ера цифрової економіки. І це вимагає суттєвої трансформації більшості економічних та інформаційних процесів в суспільстві. Увагу цифровізації та перетворенню під її впливом економічного простору в наукових працях приділяють такі науковці як К. Васюк, О. Гудзь, С. Коляденко, М. Крячко, І. Малик, Н. Мисник, Є. Підгайний, П. Стецюк, Є. Черняєв, А. Яворський та інші [1; 2].

[1] ORCID: https://orcid.org/0000-0002-1357-0497

[2] ORCID: https://orcid.org/0000-0002- 9708-7215

[3] ORCID: https://orcid.org/0000-0002-1146-2679

Фахівці досліджують більшою мірою саме впровадження цифровізації у вітчизняну економіку, приділяють увагу особливостям та можливим перешкодам в цьому процесі.

В той же час вивченням поняття та механізмів безпосередньо економічної безпеки організацій, проблематикою її забезпечення займались та займаються такі науковці як О. Ареф'єва, А. Большаков, О. Бородіна, З. Варналій, Н. Вітка, В. Геєць, Р. Дацків, Є. Діденко, С. Довбня, С. Кавун, В. Коваль, Т. Кузенко, А. Кулик, Т. Логутова, І. Маркіна, А. Нестеренко, В. Плескач, В. Пономарьов, О. Прокопішина, Н. Реверчук, І. Черняков та багато інших [3–7]. Більшість авторів-початківців розкривають теоретичні аспекти питання економічної безпеки, визнані фахівці приділяють увагу практичним аспектам забезпечення економічної безпеки, всім її складовим. Враховуючи багатогранність питання, поглиблені дослідження саме інформаційної складової представлені, на наш погляд, не в достатньому для ефективного розвитку вітчизняної економіки обсязі, особливо в умовах кризового середовища.

Тож можна стверджувати, що дослідженням інформаційної безпеки з огляду саме на бізнес-процеси, її комплексний вплив на діяльність вітчизняних організацій лише починають приділяти необхідний рівень уваги [8, с. 65]. Це відображено в змінах законодавства України, у внесенні за останні декілька років суттєвих доповнень в наявні законодавчі акти та в появі нових, які враховують зміни сучасної економіки, цифровізацію та ін. [9–15]. Кожна така зміна, а також поява нових інформаційних технологій, гаджетів, систем вимагає від організації постійного перегляду та удосконалення змісту діяльності, оновлення механізмів забезпечення економічної безпеки.

Постановка завдання. Мета даної роботи полягає в пошуку напрямів дотримання високого рівня економічної безпеки сучасної організації в умовах поєднання двох проблемних складових її практичної діяльності: необхідність забезпечувати високий рівень економічної безпеки та одночасно формувати нову систему управління з забезпеченням впровадження оптимальної цифровізації та диджиталізації.

Виклад основного матеріалу дослідження. Діяльність жодного суб'єкта господарювання не проходить без інформаційної діяльності, яку, відповідно до Закону «Про інформацію», визначають як «…створення, збирання, одержання, зберігання, використання, поширення, охорону та захист інформації» [14, Ст. 9]. Під інформацією в ньому розуміють «…будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді» [14, Ст. 1]. Частіш за все це відображення представлене у вигляді документів – «…матеріальних носіїв, що її містять та повинні забезпечити її збереження та передавання у часі та просторі» [14, Ст. 1].

Сучасні економічні відносини, глобалізація економіки, стрімкий розвиток науки, техніки та узгодження з цим законодавчої бази України поставили суб'єктів господарювання перед багатофакторними задачами. З одного боку, за законом організацію зобов'язують надавати суспільству повну інформацію про товар (роботу, послугу) [14, Ст. 14], довести їх безпеку та адекватний розмір ціни [13, Ст. 17]. Тобто, суб'єкт господарювання повинен бути максимально відкритим інформаційно перед споживачами та партнерами. Крім того, розрахункові операції, наближаючи вітчизняні організації до більш прозорого ведення бізнесу, законодавчо в 2019-2020 роках отримали доповнення правових складових електронними процесами обміну інформацією з фіскальними органами як обов'язковими [11, Ст. 2]. Для оптимізації процесу в серпні 2022 року законодавчу базу країни було доповнено сучасними визначеннями: «електронне повідомлення» та «засоби дистанційного зв'язку» [13, Ст. 1], визнаючи електронну інформацію за правовим статусом рівноправною з паперовою.

Однак одночасно з такою відкритістю на суб'єктів господарювання накладено певні вимоги щодо забезпечення збереження інформації, дотримання економічної інформаційної безпеки. І хоча теоретично за безпеку передачі інформації в мережі основна відповідальність лягає на її власника, який повинен забезпечити «здатність електронних комунікаційних мереж і послуг протистояти діям, що становлять загрозу доступності, цілісності чи конфіденційності таких мереж і послуг, а також даних, що зберігаються, передаються чи обробляються, та пов'язаних із ними послуг, що надаються або доступ до яких здійснюється через електронні комунікаційні мережі чи послуги…» [10, Ст. 2], фактично в разі витоку інформації втрати та погіршення іміджу щодо безпеки несе безпосередньо суб'єкт господарювання, чия інформація була оприлюднена. Так само при виникненні інформаційних помилок наслідки в першу чергу відчуває також суб'єкт господарювання – джерело інформації.

Тож сучасна організація стикається з наступними складностями в питаннях інформаційної економічної безпеки: необхідністю здійснювати сучасну диджиталізацію (постійно слідкувати за розвитком інформаційних технологій, відповідно до умов обирати та використовувати оптимальні для організації саме в її умовах способи приведення інформації в цифрову форму), яку визначають більш широко як «… заснований на можливостях сучасної IT-індустрії процес застосування підприємствами сучасних інформаційно-комунікаційних технологій для досягнення своєї мети, зорієнтований на трансформацію існуючих бізнес-процесів шляхом їх диджиталізації» [16, с. 19];

необхідністю здійснювати законодавчо визначений обмін інформацією з державними органами та зовнішнім середовищем на принципово новому інформаційному рівні; забезпечувати збереження та конфіденційність інформації, комерційну таємницю та її прозорість.

Розкриємо більш детально погрозу економічній безпеці організації по цим складовим. Диджиталізація має декілька прямих загроз для інформації організації. Частина з них стосується людського чиннику, частина – технічної складової процесу. Зупинимось в першу чергу на первинному рівні диджиталізації (роботі з електронними носіями інформації), та на впливі людського чиннику. Працівник, який формує електронне повідомлення, документ, може здійснити просту технічну помилку. І в разі роботи зі значним обсягом інформації помітити її вкрай складно. Тож якщо документ є базовим для формування подальших висновків, розрахунків, дій, то з наявністю цієї помилки наприкінці процесу реалізації управлінського рішення, в якому він приймав участь, може сформуватися аварійна ситуація, криза, багатотисячні збитки, а інколи й ризики загрози життю та здоров'ю людей. І якщо паперові документи зазвичай мали всього декілька копій для роботи, тож виправити знайдену помилку в усіх було не досить складно, всі попередні користувачі документу були враховані, їх попереджали про виправлення, то електронні документи в організаціях зазвичай є в одночасному доступі всіх користувачів внутрішньої мережі, тому зрозуміти – хто саме та коли користувався помилковими даними майже неможливо. Тому перевірку змушені здійснити в значно більшому обсязі. Це стримує бізнес-процес і в окремих випадках може призвести до незворотної кризи.

Ще більш складною стає ситуація, коли виправлення здійснюється в декількох документах автоматично за рахунок функції перепосилання даних в єдиній інформаційній системі. Чим довше часу проходить між появою та виявленням помилки, тим складніше виправити ситуацію. Тож проста технічна помилка може стати значною економічною загрозою.

Наступною проблемою є питання збереження або знищення інформації. Документація має чіткі законодавчо визначені терміни збереження, які для паперових носіїв інформації убезпечував в тому числі архів та інші місця їх зберігання. Однак з приходом диджиталізації окремі працівники не вважають необхідним дотримуватись термінів зберігання документів, посилаючись на обмежений обсяг місця для зберігання інформації на електронних цифрових носіях, і дозволяють собі видаляти електронні документи без узгодження терміну зберігання. Так само працівник може випадково видалити частину інформації з електронного документа або ж знищити весь документ, і тоді виправлення ситуації буде залежати від професіоналізму системного адміністратора компанії.

Крім того, в більшості організацій відсутня чітка система каталогізації електронної цифрової інформації, завдяки чому документацію, яка використовується досить не часто, через декілька років знайти вкрай складно навіть при її наявності. Проблема посилюється в разі зміни персоналу.

Ускладнення диджиталізації можуть бути спровоковані відсутністю достатнього рівня професійної та психологічної готовності персоналу до цифровізації економіки: незнання сучасних інформаційних систем, відсутність вмінь та бажання працювати з ними, відсутність знання їх відмінностей та доцільності використання, психологічне відторгнення автоматизації робочих місць та процесів тощо. Виокремимо групи проблем та їх можливе розв'язання (табл. 1).

Все це призводить до вказаних вище помилок та помилок в обранні оптимального супроводу роботи компанії, що не дає бачення дійсного змісту бізнес-процесів, збільшує час на його проектування та реалізацію, формує несучасний пакет документів, що суттєво зменшує конкурентоздатність суб'єкта господарювання.

Не менш небезпечною є ситуація, коли людський чинник втручається в інформаційні процеси в організації свідомо. Промислове шпигунство призводить до передачі секретної інформації конкурентам, ображений на керівництво та/або компанію працівник (особливо напередодні звільнення) інколи здатен оприлюднювати інформацію, яку необхідно зберігати як конфіденційну, знищувати окремі електронні документи, інколи – навмисне вносити в них помилки. Такі ситуації доводять партнерам організації та суспільству низький рівень економічної безпеки саме цього суб'єкта господарювання, що суттєво погіршує його імідж та зменшує кризостійкість.

Другу глобальну групу ризиків для економічної безпеки організації в процесі впровадження новітніх інформаційних технологій створює техніко-технологічна складова. В першу чергу необхідним є забезпечення організації відповідною технікою, яка на даний час має суттєву вартість та швидко застаріває. Тому кожен суб'єкт господарювання змушений здійснювати прогнозні розрахунки щодо доцільності впровадження сучасних інформаційних технологій в діяльність, їх окупність. При цьому зрозуміло, що їх відсутність для більшості партнерів є сигналом в недостатній платоспроможності суб'єкта, в консерватизмі або низькому рівні підготовки керівництва та персоналу тощо, що, звісно, негативно впливає на імідж.

Так само досить високу ціну має зовнішнє програмне забезпечення, ліцензійні програми тощо. Тому більшість компаній намагається для внутрішнього користування сформувати власні програмні

Таблиця 1

Ускладнення впровадження диджиталізації та цифровізації

Професійна складова	Психологічна складова
Зміст проблематики	
- незнання сучасних інформаційних систем	- відсутність бажання працювати з сучасними інформаційними системами
- відсутність вмінь працювати з сучасними інформаційними системами	- психологічне відторгнення автоматизації робочих місць
- відсутність знання їх відмінностей та доцільності використання	- психологічне відторгнення автоматизації процесів
Розв'язання наявних проблем	
Перепідготовка персоналу (в разі відсутності результату – переведення на інше робоче місце або звільнення робітника)	Психологічні тренінги (в разі відсутності результату – переведення на інше робоче місце або звільнення робітника)
Превентивні заходи	
При прийомі на роботу – випробувальне завдання	При прийомі на роботу – тестування на психологічну сумісність з діяльністю в певних умовах
До початку впровадження – навчання новітнім інформаційним можливостям з акцентом на економії зусиль, часу та збереженням рівня оплати праці; оновлення змісту корпоративної культури; формування відчуття соціальної відповідальності за впровадження новацій та ін.	

Джерело: складено авторами

продукти, які не завжди встигають в оновленні, розвитку за ринковими пропозиціями, і в певний проміжок часу втрачають сумісність та можуть призвести до втрати інформації організації або лише інформаційних каналів зв'язку з клієнтами, партнерами, фіскальними органами тощо. Тож економічна безпека організації потребує високого професіоналізму в створенні планів перспективного розвитку, в здійсненні економічного обґрунтування щодо впровадження тих чи інших інформаційних технологій, програм, обладнання (табл. 2).

Вагомою складовою економічної безпеки при роботі з інформаційними технологіями є дотримання та розвиток кібербезпеки [17], яку визначають як «…деякий стан системи, за якого нейтралізуються загрози доступності, цілісності або конфіденційності даних, що циркулюють в інформаційних системах, в тому числі кожного суб'єкта господарювання» [18, с. 499]. Вона є одночасно і складовою інформаційної безпеки суб'єкта господарювання, бо вимагає використання в інформаційних системах відповідного рівня сучасного захисту, постійного навчання персоналу для формування в них навичок безпечного поводження зі службовою інформацією; і безпосередньо процесом організації попередження та захисту від зовнішніх активних дій сторонніх щодо несанкціонованого отримання інформації від суб'єкта господарювання або задля пошкодження його інформаційних систем. Формування високого рівня кібербезпеки організації в сучасних умовах також потребує комплексного підходу до питання і керівництва, і відповідних фахівців, і кожного з працівників суб'єкта господарювання.

Оскільки зміни та розвиток складових інформаційних систем, інформаційних технологій проходить постійно, відповідно до них постійно змінюється законодавство та, нажаль, і прийоми й методи протиправних дій шахраїв та недоброзичливих осіб і компаній. Тож головним в забезпеченні економічної безпеки суб'єкта господарювання в сучасних умовах цифровізації та глобальної економіки можна вважати забезпечення безпеки інформації, каналів її зв'язку та здатність прогнозувати подальший розвиток науки, техніки, технології та законодавчої бази.

Досягти одночасно потрібного рівня цифровізації практичної діяльності та економічної безпеки організації можливо за наступних умов:

– Забезпечення постійного розвитку всього персоналу організації з питань інформаційної безпеки, для чого знайомити їх не тільки з правилами загальної безпечної роботи та поведінки, але й з практичними прикладами найновітніших шахрайських дій та схем, з прийомами та методами запобігання та нейтралізації негативних наслідків.

– Формування та жорсткий контроль за дотриманням правил безпеки роботи з інформацією та інформаційними носіями.

– Навчання відповідних працівників роботі з новаційними пропозиціями ринку інформаційних технологій.

– Формування правил найменування документів, їх каталогізації та збереження з жорстким контролем дотримання цих вимог всіма робітниками організації.

– Посилення попереднього вивчення осіб, що мають або будуть мати доступ до конфіденційної інформації.

– Розвиток кібербезпеки в організації.

– Раціональне оновлення інформаційних систем, технологій, обладнання, що буде відповідати прогнозам прибутковості діяльності організації та ін.

Таблиця 2

Група інформаційних ризиків для економічної безпеки організації

Людський чинник	Техніко-технологічна складова
- технічні помилки (загроза стримування бізнес-процесу, в окремих випадках – настання незворотної кризи)	- висока вартість техніки, яка швидко застаріває
- перепосилання помилкових даних, невідповідне збереження або знищення інформації	- висока ціна зовнішнього програмного забезпечення, ліцензійних програм тощо
- відсутність чіткої системи каталогізації електронної цифрової інформації	- різниця швидкості оновлення власних та зовнішніх програмних продуктів (призводить до неузгодженості та зупинки в роботі)
- свідоме пошкодження або знищення інформації робітниками	- технічні збої з наслідками повної або часткової втрати інформації організації
- промислове шпигунство	- технічні збої з наслідками призупинки діяльності організації

Джерело: складено авторами

Впровадження запропонованих заходів створить фундамент для подальшого розвитку сучасної інформаційної безпеки в організації, підвищить якість та стійкість бізнес-процесів та дозволить організації отримати імідж сучасного розвинутого суб'єкта господарювання.

Висновки та пропозиції. Інформація в сучасних умовах глобалізації економіки стає чи не головним ресурсом, цифровізація, диджиталізація – джерелом прибутку та нових видів діяльності. Розвиток науки, технологій, ґаджетів, інформаційних каналів змушують кожну організацію постійно адаптуватися до цих змін, розвивати та оновлювати всі ресурси. Вказані процеси постійно породжують і нові види ризиків, з якими стикається суб'єкт господарювання в своїй діяльності в інформаційному просторі. Кожен з висвітлених в статті ризиків для економічної безпеки суб'єкта господарювання потребує пошуку оптимального вирішення з урахуванням особливостей кожного підприємства, його середовища, поточного та перспективного стану розвитку інформаційних систем та інших впливових чинників, що може й повинно стати тематикою наступних досліджень.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Бензарь, А., Пєстова, О. Проблеми та перспективи розвитку цифрової економіки в Україні. *Цифрова економіка та економічна безпека.* 2022. № 2. DOI: https://doi.org/10.32782/dees.2-25.

2. Гудзь О. Цифрова економіка: зміна цінностей та орієнтирів управління підприємствами. *Економіка. Менеджмент. Бізнес.* 2018. № 2 (24). URL: http://www.dut.edu.ua/uploads/p_1010_10116202.pdf.

3. Ареф'єва О., Кузенко Т. Планування економічної безпеки підприємств. Київ : Вид-во Європ. ун-ту, 2014. 150 с.

4. Бородіна О. Оцінка економічної безпеки підприємства. Економіка: проблеми теорії та практики : зб. наук. пр. : В 3 т. Т. І. Дніпропетровськ : ДНУ, 2013. Вип. 183. С. 33–41.

5. Вороніна В., Спінжар Р. Аналіз підходів до визначення поняття економічної безпеки підприємства. Економічний форум. 2019. № 4. С. 109–115. URL: http://dspace.pdaa.edu.ua:8080/handle/123456789/6243.

6. Потапюк І., Годловський А. Теоретичні аспекти управління економічною безпекою підприємства. *Проблеми і перспективи розвитку підприємництва.* Харків : ХНАДУ, 2016. № 2 (13), т. 1. С. 25–30. URL: http://nbuv.gov.ua/UJRN/piprp_2016_2%281%29__7.

7. Потапюк, І., Мазіленко, С., Прусова, М. Фінансово-економічна безпека як основа безпеки підприємства. *Цифрова економіка та економічна безпека*. 2022. № 2. https://doi.org/10.32782/dees.2-26.

8. Дергачова В., Воржакова Ю., Хлебинська О. Організація бізнес-процесів в умовах цифровізації. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія: Міжнародні відносини. Економіка. Країнознавство. Туризм,* 2021. № 14. С.60–68. DOI: https://doi.org/10.26565/2310-9513-2021-14-06.

9. Про електронні документи та електронний документообіг. Закон України від 22.05.2003 № 851-IV зі змінами. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text.

10. Про електронні комунікації. Закон України від 16.12.2020 № 1089-IX зі змінами. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text.

11. Про застосування реєстраторів розрахункових операцій у сфері торгівлі, громадського харчування та послуг. Закон України від 06.07.1995 № 265/95-ВР зі змінами та доповненнями. URL: https://zakon.rada.gov.ua/laws/show/265/95-%D0%B2%D1%80#Text.

12. Про затвердження Порядку роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання. Наказ Міністерства юстиції України від 11.11.2014 № 1886/5 зі змінами. URL: https://zakon.rada.gov.ua/laws/show/z1421-14#Text.

13. Про захист прав споживачів. Закон України від 12.05.1991 № 1023-XII зі змінами та доповненнями. URL: https://zakon.rada.gov.ua/laws/show/1023-12?find=1&text=%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5#Text.

14. Про інформацію. Закон України від 02.10.1992 № 2657-XII зі змінами та доповненнями. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

15. Про стимулювання розвитку цифрової економіки в Україні. Закон України від 15.07.2021 № 1667-IX. URL: https://zakon.rada.gov.ua/laws/show/1667-20#Text.

16. Гудзь О., Федюнін С., Щербина В. Диджиталізація, як конкурентна перевага підприємств. *Економіка. Менеджмент. Бізнес*. 2019. № 3 (29). С. 18–24. http://doi.org/10.31673/2415-8089.2019.031824.

17. Маковець О., Дрозд І. Кібербезпека як фактор фінансової безпеки підприємства. *Економіка. Фінанси. Право*. 2020. № 5/3. С. 31–35. https://doi.org/10.37634/efp.2020.5(3).8.

18. Вітер С., Світлишин І. Захист облікової інформації та кібербезпека підприємства. *Економіка і суспільство.* 2017. Випуск 11. С.497–502. URL: https://economyandsociety.in.ua/journals/11_ukr/80.pdf.

REFERENCES:

1. Benzar, A., Piestova, O. (2022) Problemy ta perspektyvy rozvytku tsyfrovoi ekonomiky v Ukraini [Problems and prospects for the development of the digital economy in Ukraine]. *Tsyfrova ekonomika ta ekonomichna bezpeka*, no. 2. DOI: https://doi.org/10.32782/dees.2-25.

2. Hudz O. (2018) Tsyfrova ekonomika: zmina tsinnostei ta oriientyriv upravlinnia pidpryiemstvamy [Digital economy: changing values and orientations of enterprise management]. *Ekonomika. Menedzhment. Biznes*, no. 2 (24). Available at: http://www.dut.edu.ua/uploads/p_1010_10116202.pdf.

3. Arefieva O., Kuzenko T. (2014) Planuvannia ekonomichnoi bezpeky pidpryiemstv [Planning of economic security of enterprises]. Kyiv: Vyd-vo Yevrop. un-tu, 150 p.

4. Borodina O. (2013) Otsinka ekonomichnoi bezpeky pidpryiemstva. Ekonomika: problemy teorii ta praktyky : zb. nauk. pr. : V 3 t. [Assessment of economic security of the enterprise. Economics: problems of theory and practice: coll. of science pr.: In 3 vols]. Dnipropetrovsk: DNU, vol. 183, pp. 33–41.

5. Voronina V., Spinzhar R. (2019) Analiz pidkhodiv do vyznachennia poniattia ekonomichnoi bezpeky pidpryiemstva [Analysis of approaches to defining the concept of economic security of the enterprise]. *Ekonomichnyi forum*, no. 4, pp. 109–115. Available at: http://dspace.pdaa.edu.ua:8080/handle/123456789/6243.

6. Potapiuk I., Hodlovskyi A. (2016) Teoretychni aspekty upravlinnia ekonomichnoiu bezpekoiu pidpryiemstva [Theoretical aspects of managing the economic security of the enterprise]. *Problemy i perspektyvy rozvytku pidpryiemnytstva*, no. 2 (13), vol. 1, pp. 25–30. Available at: http://nbuv.gov.ua/UJRN/piprp_2016_2%281%29__7.

7. Potapiuk, I., Mazilenko, S., Prusova, M. (2022) Finansovo-ekonomichna bezpeka yak osnova bezpeky pidpryiemstva [Financial and economic security as the basis of enterprise security]. *Tsyfrova ekonomika ta ekonomichna bezpeka*, no. 2. DOI: https://doi.org/10.32782/dees.2-26.

8. Derhachova V., Vorzhakova Yu., Khlebynska O. (2021) Orhanizatsiia biznes-protsesiv v umovakh tsyfrovizatsii [Organization of business processes in conditions of digitalization]. *Visnyk Kharkivskoho natsionalnoho universytetu imeni V. N. Karazina. Seriia: Mizhnarodni vidnosyny. Ekonomika. Krainoznavstvo. Turyzm*, no. 14, pp. 60–68. DOI: https://doi.org/10.26565/2310-9513-2021-14-06.

9. Pro elektronni dokumenty ta elektronnyi dokumentoobih. Zakon Ukrainy vid 22.05.2003 № 851-IV zi zminamy [About electronic documents and electronic document flow. Law of Ukraine dated 05/22/2003 No. 851-IV as amended]. Available at: https://zakon.rada.gov.ua/laws/show/851-15#Text.

10. Pro elektronni komunikatsii. Zakon Ukrainy vid 16.12.2020 № 1089-IX zi zminamy [About electronic communications. Law of Ukraine dated 16.12.2020 No. 1089-IX as amended]. Available at: https://zakon.rada.gov.ua/laws/show/1089-20#Text.

11. Pro zastosuvannia reiestratoriv rozrakhunkovykh operatsii u sferi torhivli, hromadskoho kharchuvannia ta posluh. Zakon Ukrainy vid 06.07.1995 № 265/95-VR zi zminamy ta dopovnenniamy [On the use of registrars of settlement operations in the sphere of trade, catering and services. Law of Ukraine dated 07/06/1995 No. 265/95-BP as amended]. Available at: https://zakon.rada.gov.ua/laws/show/265/95-%D0%B2%D1%80#Text.

12. Pro zatverdzhennia Poriadku roboty z elektronnymy dokumentamy u dilovodstvi ta yikh pidhotovky do peredavannia na arkhivne zberihannia. Nakaz Ministerstva yustytsii Ukrainy vid 11.11.2014 № 1886/5 zi zminamy [On approval of the Procedure for working with electronic documents in record keeping and their preparation for transfer to archival storage. Order of the Ministry of Justice of Ukraine dated 11.11.2014 No. 1886/5 with changes]. Available at: https://zakon.rada.gov.ua/laws/show/z1421-14#Text.

13. Pro zakhyst prav spozhyvachiv. Zakon Ukrainy vid 12.05.1991 № 1023-XII zi zminamy ta dopovnenniamy [On the protection of consumer rights. Law of Ukraine dated 12.05.1991 No. 1023-XII as amended]. Available at: https://zakon.rada.gov.ua/laws/show/1023-12?find=1&text=%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5#Text.

14. Pro informatsiiu. Zakon Ukrainy vid 02.10.1992 № 2657-XII zi zminamy ta dopovnenniamy [About information. Law of Ukraine dated 02.10.1992 No. 2657-XII as amended]. Available at: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

15. Pro stymuliuvannia rozvytku tsyfrovoi ekonomiky v Ukraini. Zakon Ukrainy vid 15.07.2021 № 1667-IX [On stimulating the development of the digital economy in Ukraine. Law of Ukraine dated 15.07.2021 No. 1667-IX]. Available at: https://zakon.rada.gov.ua/laws/show/1667-20#Text.

16. Hudz O., Fediunin S., Shcherbyna V. (2019) Dydzhytalizatsiia, yak konkurentna perevaha pidpryiemstv [Digitalization as a competitive advantage of enterprises]. *Ekonomika. Menedzhment. Biznes*, no. 3 (29), pp. 18–24. DOI: http://doi.org/10.31673/2415-8089.2019.031824.

17. Makovets O., Drozd I. (2020) Kiberbezpeka yak faktor finansovoi bezpeky pidpryiemstva [Cybersecurity as a factor in the financial security of an enterprise]. *Ekonomika. Finansy. Pravo*, no. 5/3, pp. 31–35. DOI: https://doi.org/10.37634/efp.2020.5(3).8.

18. Viter S., Svitlyshyn I. (2017) Zakhyst oblikovoi informatsii ta kiberbezpeka pidpryiemstva [Protection of accounting information and enterprise cyber security]. *Ekonomika i suspilstvo*, vol. 11, pp. 497–502. Available at: https://economyandsociety.in.ua/journals/11_ukr/80.pdf.