DOI: https://doi.org/10.32999/ksu2307-8030/2024-52-3

УДК 338.246:[005.934:316.774:351.863(477)

Черв'як А.В.
доктор філософії, учений секретар
Національного університету
«Полтавська політехніка імені Юрія Кондратюка»
ORCID: https://orcid.org/0000-0002-2747-4041
E-mail: anncherviak@gmail.com

Буряк А.А.
кандидат економічних наук, доцент,
доцент кафедри фінансів, банківського бізнесу
та оподаткування
Національного університету
«Полтавська політехніка імені Юрія Кондратюка»
ORCID: https://orcid.org/0000-0002-0814-7459
E-mail: a_buriak@ukr.net

Циганенко К.Д.
аспірант кафедри фінансів, банківського бізнесу
та оподаткування
Національного університету
«Полтавська політехніка імені Юрія Кондратюка»
ORCID: https://orcid.org/0009-0004-1580-253X
E-mail: kyrylts5991@gmail.com

ОСОБЛИВОСТІ ФОРМУВАННЯ БЕЗПЕКООРІЄНТОВАНОГО ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА НАЦІОНАЛЬНОЇ ЕКОНОМІКИ

У статті досліджено питання принципів формування безпекоорієнтованого інформаційного середовища національної економіки. За використання методів збору та обробки інформації досліджено таксономію даного поняття, сформовано його зміст та значення. Сформовано структуру безпекоорієнтованого інформаційного середовища національної економіки де виділено п'ять ключових елементів. Визначено принципи формування безкоорієнтованого інформаційного середовища, дотримання яких забезпечуватиме раціональну діяльність й ефективне виконання поставлених завдань. Визначено вектори й цілі розвитку безпекоорієнтованого інформаційного середовища з урахуванням становлення Індустрії 4.0. Охарактеризовано бачення подальшого розвитку безпекоорієнтованого інформаційного середовища для підвищення економічної безпеки України, враховуючи особливості і цінності Індустрії 5.0, особливо у воєнний та повоєнний періоди.

Ключові слова: безпекоорієнтоване інформаційне середовище, інформаційна безпека, національна безпека, національна економіка.

Cherviak Anna, Buriak Alona, Tsyhanenko Kyryl. FEATURES OF FORMATION SECURITY-ORIENTED INFORMATION ENVIRONMENT OF THE NATIONAL ECONOMY

The economic and political situation that has formed in Ukraine today, the revolutionary and military events of recent years have caused dynamic changes in the state, especially this has affected its security. Ukraine is integrating into the concept of the fourth industrialization (Industry 4.0), which involves the digitization of production, the introduction of automated systems, artificial intelligence, the development of the IT sector and robotics. Industry 4.0 opens up new opportunities for economic growth, but in turn requires the formation of a security-oriented information environment of the national economy. Information is currently a strategically important management resource. The article examines the issue of the principles of forming a security-oriented information environment of the national economy. Using methods of information collection and processing, the taxonomy of this concept was studied, its content and meaning were formed. The structure of the security-oriented information environment of the national economy was formed, where five key elements were highlighted. The principles of the formation of an uncoordinated information environment have been determined, the observance of which will ensure rational activity and effective performance of assigned tasks. It was determined that the principles of building a security-oriented information environment of the national economy are focused on protection against cyber threats and information attacks. They include strengthening cyber security, controlling access to data, protecting critical facilities and implementing information security strategies. Strategic planning and international cooperation are identified as important elements that will help reduce risks in the digital economy, especially in the conditions of globalization and modern conflicts. The vectors and guidelines for the development of a security-oriented information environment, taking into account

the development of Industry 4.0, are identified. The vision of the further development of a security-oriented information environment to increase the economic security of Ukraine is characterized, taking into account the features and values of Industry 5.0, especially in the war and post-war periods.

Key words: security-oriented information environment, information security, national security, national economy.

Постановка проблеми. Україна інтегрується в концепцію четвертої індустріалізації (Індустрія 4.0), яка передбачає цифровізацію виробництва, впровадження автоматизованих систем, штучного інтелекту, розвиток IT-сектору та робототехніки. Індустрія 4.0 відкриває нові можливості для економічного зростання, проте в свою чергу вимагає формування безпекоорієнтованого інформаційного середовища національної економіки. Інформація наразі є стратегічно важливим управлінським ресурсом. Проведення виваженої інформаційної політики суттєво впливає на вирішення внутрішньо- та зовнішньополітичних питань й військових конфліктів, що важливо для України у сучасних умовах. Отже, потрібно підійти до розгляду питання формування безпекоорієнтованого інформаційного середовища національної економіки, що будуть базуватися на ключових положеннях вирішення військових конфліктів та Індустрії 4.0.

Аналіз останніх досліджень і публікацій. У контексті Індустрії 4.0, активної цифровізації та зростання загроз в інформаційному просторі особливо гостро стоїть питання формування безпекоорієнтованого інформаційного середовища національної економіки. Значна кількість наукових досліджень з даної тематики доводять її актуальність. Проблеми захисту інформаційного простору держави та забезпечення високого рівня інформаційної безпеку, як основну складову національної безпеки розглядали у своїх наукових дослідженнях Варналій З.С. [1], Войко О.В. [2], Войціховський А.В. [3], Ільницька У. [4], Муравська Ю.Є. [5], Онищенко С.В. [6], Панченко О.А. [7], Федорова Н.Є. [8] та ін.

Метою статті є дослідження таксономії термінології безпекоорієнтованого інформаційного середовища та визначення принципів його формування.

Виклад матеріалу дослідження та його основні результати. Сучасний стан національної економіки України в безпековому аспекті характеризується високим рівнем загроз, пов'язаних з війною, кібернападами, інформаційними атаками та економічними санкціями. Збройний конфлікт підвищує ризики для критичної інфраструктури та економічних ресурсів, особливо в енергетичній, фінансовій та транспортній сферах. Для зменшення цих загроз Україна активно розвиває систему кібербезпеки, вдосконалює законодавчу базу та інтегрує міжнародні стандарти безпеки для протидії як внутрішнім, так і зовнішнім загрозам.

В умовах четвертої промислової революції (Індустрія 4.0) інформаційна безпека стає найбільш важливим і самостійним елементом у національній економіці. Індустрія 4.0. охоплює автоматизацію та цифровізацію виробничих процесів за допомогою сучасних технологій та буквально означає злиття технологій, що розмиває межі між фізичною, цифровою та біологічною сферами [9]. Це призводить до підвищення ефективності взаємодії всіх суб'єктів національної економіки та відкриває нові можливості для бізнесу. Поряд з тим, це призводить до поглиблення інформатизації економічних процесів та встановлення тісної взаємозалежності національної економіки та національної безпеки з інформаційним середовищем та його безпековим аспектом. Це є результатом того, що інформація у її первинному вигляді стала товаром і стратегічно важливим ресурсом, який забезпечує розвиток економіки та ринку інформаційних послуг. Ці всі аспекти надають зростаючої питомої ваги інформаційно-комунікаційному сектору економіки [10; 11].

Інформація є стратегічним національним ресурсом від рівня захищеності якої залежить рівень національної безпеки. Конституцією України визначено, що найважливішими функціями держави та загальносуспільним інтересом жителів країни є забезпечення економічної безпеки та інформаційного середовища держави, беззаперечний захист суверенітету України та дотримання принципу, згідно з яким територія держави є неподільною та єдиною [12].

Враховуючи вищезазначене необхідно дослідити таксономію термінології безпекоорієнтованого інформаційного середовища національної економіки для подальшого визначення векторів й орієнтирів розвитку безпекоорієнтованого інформаційного середовища та принципів його формування.

Для того, щоб сформувати об'єктивне поняття безпекоорієнтованого інформацій-

ного середовища, перш за все, необхідно проаналізувати базові підходи до визначення поняття інформаційної безпеки в економічній літературі, що наведено у табл. 1.

Безпекоорієнтоване інформаційне середовище включає у свою структуру не тільки інформаційну безпеку, але й загальні стратегії захисту національної економіки, критичної інфраструктури, а також нормативно-правове регулювання та міжнародну співпрацю у сфері безпеки.

Отже, проаналізувавши законодавчу базу та підходи вчених до визначення поняття інформаційна безпека, враховуючи специфіку даного поняття, під безпекоорієнтованим інформаційним середовищем національної економіки пропонуємо розуміти сукупність методів, технологій і заходів, спрямованих на забезпечення захисту інформаційних ресурсів усіх галузей національної економіки, критичної інфраструктури та стратегічно важливих об'єктів від внутрішніх і зовнішніх дестабілізуючих факторів. Дане поняття включає в себе управління інформаційними каналами, контроль допуску до інформації, кіберзахист що унеможливлює витік інформації, проведення маніпуляційних дій з даними та хакерські атаки на програми обслуговування та бази даних.

Відповідно до сформульованого визначення, доцільно виділити напрями формування безпекоорієнтованого інформаційного середовища національної економіки, які наведено на рис. 1.

Нормативно-правове регулювання представляє собою закони, нормативні акти, положення та стратегії що стосуються регулювання інформаційної безпеки на мікро-, мезо- та макро рівнях.

Кібербезпека як елемент безпекоорієнтованого інформаційного середовища – це захист інформаційних каналів, баз даних та систем від зовнішніх та внутрішніх дестабілізуючих факторів. Це можуть бути шпигунство чи зловмисне втручання, зловживання доступом або помилки співробітників.

У структурі безпекоорієнтованого інформаційного середовища захист критичної інфраструктури передбачає захист стратегічно важливих об'єктів пов'язаних із забезпеченням безперебійної роботи електростанцій, ядерних установок, транспортних сполучень і фінансових систем, що є критичними для функціонування націо-

Таблиця 1

Підходи до визначення поняття «інформаційна безпека»

Автор	Зміст поняття
Стратегія інформаційної безпеки [13]	Ключова складова національної безпеки України; рівень захищеності суверенітету, цілісності території, демократичного конституційного устрою та інших стратегічно необхідних інтересів держави, суспільства та кожної окремої особистості при якому цілком і повністю забезпечено конституційні права та свободу людини на будь які дії (поширення, зберігання чи використання) з інформаційними даними й надано доступ до об'єктивної та перевіреної інформації. Для створення відповідних передумов забезпечення інформаційної безпеки створена дієва система захисту та превентивних заходів спрямованих на протидію неправомірним та несанкціонованим діям в інформаційному середовищі: поширення недостовірної інформації чи деструктивної пропаганди, несанкціонованого доступу до даних з обмеженим доступом чи персональних даних людей, порушення цілісності інформації шляхом неповного її трактування.
Богуш В.М., Юдін О.К. [14]	Забезпечення відповідного рівня безпеки інформаційного середовища, що передбачає створення та використання потенційних можливостей для розвитку, незалежно від дії на нього дестабілізуючих факторів будь якого характеру походження, та не суперечить стратегічним цілям та інтересам держави.
Барановський О.І. [15]	стан захищеності інтересів держави в інформаційному просторі при якому можливість завдати шкоди державі чи суспільству зводиться до мінімального рівня чи не допускається взагалі. Негативний вплив на рівень інформаційної безпеки може бути результатом розповсюдження недостовірної та неповної інформації, через поширення та використання неперевіреної інформації чи здобутої неправомірним шляхом.
Сороківська О.А. [16]	Забезпечення такого рівня суспільних відносин, які формують та підтримують на високому рівні діяльність інформаційних систем суб'єкта господарювання.
Горбатюк О.М. [17]	Рівень захищеності інформаційних потреб особи, суспільства та держави, який гарантує їхнє існування і поступовий розвиток, незважаючи на інформаційні загрози внутрішнього чи зовнішнього походження.

Джерело: узагальнено авторами

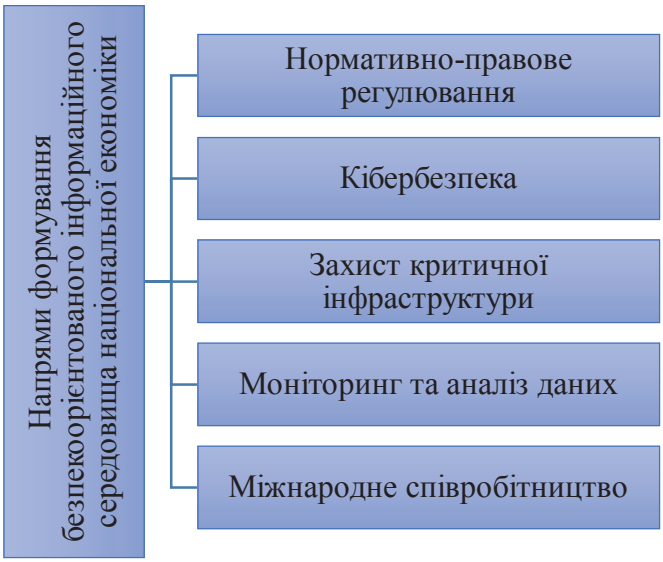

Рис. 1. Напрями формування безпекоорієнтованого інформаційного середовища національної економіки

Джерело: складено авторами

нальної економіки і безпеки. Даний елемент у структурі винесено окремо, оскільки в умовах розпочатого повномасштабного вторгнення рф в Україну ведеться гібридна війна, яка направлена дестабілізувати інформаційний простір України, розбалансувати комунікацію між об'єктами критичної інфраструктури завдавши глобальних наслідків для всієї життєзабезпечувальної системи країни [18].

Моніторинг та аналіз даних – це комплекс заходів та систем для аналізу зовнішнього та внутрішнього інформаційного середовища, відстеження потенційних та наявних загроз та прийняття оперативних рішення з реагування на дистабілізуючі фактори.

Міжнародна співпраця передбачає обмін досвідом та об'єднання зусиль з партнерами для боротьби з глобальними інформаційними викликами.

Для раціональної організації безкоорієнтованого інформаційного середовища й ефективного виконання поставлених до нього завдань необхідно спиратися на відповідні принципи. У затвердженій у 2021 році Стратегії інформаційної безпеки визначено 7 стратегічних цілей та напрямів реалізації Стратегії [13]. Згідно з даного нормативного документу стійкість і взаємодія виступають основними напрямами у забезпеченні інформаційної безпеки України. Відповідно для досягнення поставлених завдань Стратегії необхідно дотримуватися стратегічних цілей та завдань.

Відповідно до визначених стратегічних цілей пропонуємо виділяти наступні принципи формування безпекоорієнтованого інформаційного середовища національної економіки.

– системності, що передбачає формування безпекоорієнтованого інформаційного середовища як складної динамічної системи, тобто сукупності елементів (інформації, методів і прийомів аналізу, вихідних документів, фахівців тощо), котрі знаходяться у взаємозв'язку, взаємозалежності та створюють відповідну цілісність;

– прозорості, який полягає у контролі інформаційних процесів за дотриманням чинного законодавства;

– сумісності, відповідно до якого при формуванні безпекоорієнтованого інформаційного середовища повинні бути створені інформаційні інтерфейси й встановлені правила взаємодії з іншими складовими;

– гнучкості (адаптивності), що полягає у можливості швидкої адаптації інформаційного середовища до змін зовнішнього та внутрішнього середовища без суттєвої модифікації методів і засобів збирання інформації та проведення аналітичної роботи;

– обґрунтованості, шо вимагає надання аргументованих результатів аналітичної роботи на основі використання сучасних наукових підходів, аналітичних прийомів та інформаційних технологій тощо;

– проактивності, відповідно до якого функціонування безпекоорієнтованого

інформаційного середовища повинно бути спрямовано на проведення досліджень й формування результатів незалежно від конкретних запитів користувачів, що передбачає роботу на випередження з елементами прогнозування;

– стандартизації, який передбачає застосування типових, стандартизованих елементів, рішень, процесів, прикладних програм для вирішення якомога ширшого кола завдань;

– постійного розвитку, що вимагає, поряд з використанням стандартизованих елементів, регулярної актуалізації інформаційного середовища на основі останніх досягнень науки та інформаційно-комп'ютерних технологій без порушення процесу його функціонування;

– ефективності, який передбачає досягнення оптимального співвідношення між витратами й цільовими результатами;

– пріоритетності, який полягає у першочерговості захисту стратегічних об'єктів та суб'єктів критичної інфраструктури.

Принципи побудови безпекоорієнтованого інформаційного середовища національної економіки зосереджені на захисті від кіберзагроз та інформаційних атак. Вони включають зміцнення кібербезпеки, контроль доступу до даних, охорону критичних об'єктів і впровадження стратегій інформаційної безпеки. Важливими елементами є стратегічне планування та міжнародна співпраця, що сприяють зменшенню ризиків у цифровій економіці, особливо в умовах глобалізації та сучасних конфліктів [19].

Розвиток безпекоорієнтованого інформаційного середовища з урахуванням становлення Індустрії 4.0 передбачає адаптацію до нових технологічних викликів, таких як автоматизація виробництва, штучний інтелект (ШІ), інтернет речей і великі дані. Це вимагає підвищення рівня кібербезпеки та захисту даних, інтеграції систем моніторингу загроз, а також розробки нормативної бази для регулювання нових технологій. Забезпечення безпеки в умовах Індустрії 4.0 стає важливим елементом стійкого розвитку національної економіки та захисту критичної інфраструктури.

На законодавчому рівні в Україні прийняті відповідні рішення, що стосуються безпекоорієнтованого інформаційного середовища країни. Згідно з Розпорядження Кабінету Міністрів України, 6 грудня 2017 року було ухвалено Концепцію створення державної системи захисту критичної інфраструктури, ключовою позицією якої є забезпечення системи захисту критичної інфраструктури [20]. У Концепції визначено ключові напрямки, механізми, шляхи і способи розв'язання проблем пов'язаних із захистом критичної інфраструктури.

Індустрія 4.0 створила основу для автоматизації та обміну даними у виробничих процесах. Однак лідери промисловості вже готуються до Індустрії 5.0, яка зосереджується на людині як ключовому елементі виробничих процесів. Це допоможе знизити страх перед технологічним безробіттям, викликаним автоматизацією Індустрії 4.0, і зменшить спротив до впровадження нових технологій, роблячи їх більш гуманізованими та спрямованими на співпрацю між людиною і машинами [21].

Роль та значення безпекоорієнтованого інформаційного середовища національної економіки в Індустрії 5.0 буде мати таке ж стратегічно важливе значення як і при Індустрії 4.0. Воно буде забезпечувати захист даних і безперебійну взаємодію між людиною та машинами. В умовах, коли індивідуалізовані виробничі процеси все більше залежать від штучного інтелекту та роботизованих процесів, інформаційна безпека запобігає кібератакам, витоку конфіденційної інформації та саботажу систем. Це включає контроль доступу, шифрування даних, а також впровадження стандартів кібербезпеки для захисту від нових ризиків у цифрових екосистемах.

Отже незалежно від етапу реалізації четвертої чи п'ятої промислової революції поняття інформації та інформаційної безпеки продовжує бути стратегічно важливим у національній економіці та безпеці.

Висновки. Отже, в умовах сучасного інформаційного розвитку суспільства, ведення гібридного характеру війни рф проти України захист національного інформаційного простору та інформаційна безпека є ключовим пріоритетом для національної безпеки. При цьому безпекоорієнтоване інформаційне середовище національної економіки варто розглядати як самостійний елемент системи безпеки, що відображає її стратегічне значення для державного розвитку та захисту від загроз.

Забезпечення інформаційної безпеки є критично важливим для України, оскільки країна стикається з постійними загрозами в інформаційному просторі. Визначені принципи формування безпекоорієнтованого інформаційного середовища національної економіки зосереджені на

захисті від кіберзагроз та інформаційних атак. Вони стосуються ключових аспектів зміцнення кібербезпеки, контроль доступу до даних, охорону критичних об'єктів і впровадження стратегій інформаційної безпеки.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Варналій З.С., Онищенко С.В., Маслій О.А. Загрози економічній безпеці України в умовах глобалізації. Конкурентні стратегії безпеки розвитку України у глобальному середовищі: монографія. / за заг. ред. А.І. Мокія. ДУ «Інститут регіональних досліджень імені М.І. Долішнього НАН України». Львів, 2019. С. 21–95.
2. Войтко О.В. Реалізація державної інформаційної політики та забезпечення інформаційної безпеки в умовах конфлікту з Російською Федерацією. *Міжнародний журнал «Грааль науки»*. 2021. № 1. С. 164–166.
3. Войціховський А. В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Право»*. 2020. № 29. С. 281–288.
4. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Політичні науки.* 2016. Вип. 2 (1). С. 27–32.
5. Муравська (Якубівська) Ю.Є. Інформаційна безпека суспільства: концептуальний аналіз. *Економіка і суспільство*. 2017. Вип. 9. С. 289–29
6. Онищенко С.В., Білько С.С. Концепти синергетичного підходу до формування безпекоорієнтованого інформаційного середовища в Україні. *Вісник Хмельницького національного університету.* 2023. № 1 (314). С. 204–211.
7. Панченко О.А. Інформаційна безпека в епоху турбулентності: державно-управлінський аспект: монографія. Київ : КВІЦ, 2020. 332 с.
8. Федорова Н.Є., Смєсова В.Л. Інформаційна безпека та шляхи її забезпечення на етапі інформаційно-технологічної революції. *Причорноморська економічні студії*. 2020. Вип. 57. С. 13–16.
9. Klaus Schwab. 4 Industrial Revolution: what it means, how to respond. WEF. URL: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond (дата звернення 20.09.2024).
10. Гнатенко В. Основні складові економічної безпеки держави. *Науковий вісник : Державне управління*. 2021. № 1 (7). С. 66–82.
11. Маслій О.А., Максименко А.П. Ризики та загрози економічній безпеці України у цифровій сфері в умовах війни. *Ринкова економіка: сучасна теорія і практика управління*. 2023. Том 21 № 3(52). С. 179–199.
12. Конституція України. Сервіс документів. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення 22.09.2024).
13. Стратегія інформаційної безпеки. Сервіс документів. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення 22.09.2024).
14. Богуш В.М., Юдін О.К. Інформаційна безпека держави. Київ : «МК-Прес», 2005. 432 с.
15. Барановський О. І. Фінансова безпека. Київ : Фенікс, 1999. 338 с.
16. Сороківська О.А., Гевко В.Л. Інформаційна безпека підприємства: нові загрози та перспективи. *Економічні науки: Вісник Хмельницького національного університету.* 2010. № 2. Т. 2. С. 32–35.
17. Горбатюк О.М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть. *Вісник Київського університету імені Т. Шевченка*. 1999. Вип. 14. С. 46–48
18. Онищенко С.В., Маслій О.А., Глушко А.Д., Загорулько Т.А. Виклики та загрози соціально-економічній безпеці України в умовах воєнного стану. *Економіка і регіон*. 2023. № 1 (88). С. 135–143.
19. Buriak A., Masliy O. Strategic foundations of security-oriented international space: economic, informational and ecological dimensions. *Economics and Region*. 2024. № 1 (92). С. 281–286.
20. 20. Концепція створення державної системи захисту критичної інфраструктури. Сервіс документів. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text (дата звернення 21.09.2024).
21. Ривак Н. О. Індустрія 5.0: перехід до стійкої та орієнтованої на людину промисловості. *Соціально-економічні проблеми сучасного періоду України*. 2022. Вип. 3(155). С. 41–46.

REFERENCES:

1. Varnalii Z. S., Onyshchenko S. V., Maslii O. A. (2019) Threats to the economic security of Ukraine in the conditions of globalization. Competitive security strategies of Ukraine's development in the global environment: monograph / in general ed. A. I. Mokiya. State University “Institute of Regional Studies named after M.I. Dolishnyo National Academy of Sciences of Ukraine”. Lviv. P. 21–95.
2. Voitko O. V. (2021) Implementation of the state information policy and provision of information security in the conditions of the conflict with the Russian Federation. *International journal “Grail of Science”*, no. 1, pp. 164–166.
3. Voytsikhovsky A. V. (2020) Information security as a component of the national security system (international and foreign experience). *Bulletin of Kharkiv National University named after V. N. Karazin. “Law” series*, no. 29, pp. 281–288.
4. Ilnytska U. (2016) Information security of Ukraine: modern challenges, threats and countermeasures against negative information and psychological influences. *Political sciences*, issue 2 (1), pp. 27–32.
5. Muravska (Yakubivska) Yu. E. (2017) Information security of society: a conceptual analysis. *Economy and society*, issue 9, pp. 289–29
6. Onishchenko S. V., Bilko S. S. (2023) Concepts of a synergistic approach to the formation of a security-oriented information environment in Ukraine. *Bulletin of the Khmelnytskyi National University*, no. 1 (314), pp. 204–211.
7. Panchenko O. A. (2020)Information security in the era of turbulence: state-management aspect: monograph. Kyiv: KVITS, 332 p.
8. Fedorova N. E., Smyesova V. L. (2020) Information security and ways to ensure it at the stage of the information technology revolution. *Black Sea Economic Studies*, issue 57, pp. 13–16.

9. Klaus Schwab. 4 Industrial Revolution: what it means, how to respond. WEF. Available at: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond (accessed September 20, 2024).
10. Hnatenko V. (2021) The main components of the economic security of the state. *Scientific Bulletin: State Administration*, no. 1 (7), pp. 66–82.
11. Maslii O. A., Maksymenko A. P. (2023) Risks and threats to the economic security of Ukraine in the digital sphere in the conditions of war. *Market economy: modern management theory and practice*, volume 21, no. 3(52), pp. 179–199.
12. Constitution of Ukraine. Document service. Available at: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (accessed September 22, 2024).
13. Information security strategy. Document service. Available at: https://zakon.rada.gov.ua/laws/show/685/2021#Text (accessed September 22, 2024).
14. Bogush V. M., Yudin O. K. (2005) Information security of the state. Kyiv: MK-Press, 432 p.
15. Baranovsky O. I. (1999) Financial security. Kyiv: Phoenix, 338 p.
16. Sorokivska O. A., Gevko V. L. (2010) Enterprise information security: new threats and prospects. *Economic Sciences: Bulletin of the Khmelnytskyi National University*, no. 2, vol. 2, pp. 32–35.
17. Horbatyuk O. M. (1999) The current state and problems of information security in Ukraine at the turn of the century. *Bulletin of Kyiv University named after T. Shevchenko*, vol. 14, pp. 46–48
18. Onyshchenko S. V., Masliy O. A., Glushko A. D., Zagorulko T. A. (2023) Challenges and threats to the socio-economic security of Ukraine in the conditions of martial law. *Economy and the region*, no. 1 (88), pp. 135–143.
19. Buriak A., Masliy O. (2024) Strategic foundations of security-oriented international space: economic, informational and ecological dimensions. *Economics and Region*, no. 1 (92), pp. 281–286.
20. The concept of creating a state system for the protection of critical infrastructure. Document service. Available at: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text (accessed September 21, 2024).
21. Ryvak N. O. (2022) Industry 5.0: transition to a sustainable and human-oriented industry. Socio-economic problems of the modern period of Ukraine, issue 3(155), pp. 41–46.

Стаття надійшла до редакції 27.09.2024.
The article was received 27 September 2024.