DOI: [10.32702/2307-2105-2022.2.95](https://doi.org/10.32702/2307-2105-2022.2.95)

УДК: 338.2

А. Д. Глушко,

к. е. н., доцент,

Національний університет «Полтавська політехніка імені Юрія Кондратюка», Україна

ORCID ID: 0000-0002-4086-1513

В. В. Пантась,

студентка 4 курсу,

Національний університет «Полтавська політехніка імені Юрія Кондратюка», Україна

ORCID ID: 0000-0002-72416238

С. Р. Бабенко,

студентка 4 курсу,

Національний університет «Полтавська політехніка імені Юрія Кондратюка», Україна

ORCID ID: 0000-0003-3894-0500

ІНФОРМАЦІЙНА ПОЛІТИКА В СИСТЕМІ ЗАБЕЗПЕЧЕННЯ ФІНАНСОВОЇ БЕЗПЕКИ ДЕРЖАВИ

A. Hlushko

PhD in Economics, Associate Professor,

National University «Yuri Kondratyuk Poltava Polytechnic»

V. Pantas

4th year student,

National University «Yuri Kondratyuk Poltava Polytechnic»

S. Babenko

4th year student,

National University «Yuri Kondratyuk Poltava Polytechnic»

INFORMATION POLICY IN THE SYSTEM OF FINANCIAL SECURITY OF THE STATE

У статті актуалізована проблематика підвищення ефективності інформаційної політики України в аспекті забезпечення її фінансової безпеки. У дослідженні представлено систему інформаційної політики, з урахуванням взаємозв'язків між складовими елементами. Обґрунтовано значення інформаційної політики в системі забезпечення фінансової безпеки України. Саме інформаційна політика, яка надає можливість громадянам, суб'єктам господарювання та державі протистояти небезпекам та загрозам, що можуть завдати фінансової шкоди, визначена одним із головних складових системи забезпечення фінансової безпеки держави.

Встановлено, що головною метою державної інформаційної політики в сучасних умовах є якісне інформаційне забезпечення стратегічних і оперативних завдань соціально-економічного розвитку держави, створення інформаційно стійкого до зовнішніх та внутрішніх загроз суспільства. Офіційними статистичними даними підтверджено

негативну динаміку зростання рівня ризиків та загроз в інформаційній сфері, які спричинили величезні фінансові втрати, та негативно вплинули на рівень фінансової безпеки країни. Проведено дослідження досвіду провідних країн світу у сфері реалізації інформаційної політики та виокремлено можливості впровадження в Україні. Визначено пріоритетні напрями інформаційної політики в контексті забезпечення фінансової безпеки, ефективність яких буде максимальною за умови комплексності та системності їх реалізації.

The article highlights the issue of improving the effectiveness of information policy of Ukraine in terms of ensuring its financial security. The study presents an information policy system, taking into account the relationships between the constituent elements. The importance of information policy in the system of financial security of Ukraine is substantiated. It is the information policy that enables citizens, businesses and the state to confront the dangers and threats that can cause financial damage, identified as one of the main components of the system of financial security of the state. It is established that the main goal of the state information policy in modern conditions is high-quality information support of strategic and operational tasks of social and economic development of the state, creation of information resistant to external and internal threats of society. Official statistics confirm the negative dynamics of the growth of risks and threats in the information sphere, which caused huge financial losses and negatively affected the level of financial security of the country. The analysis shows that the landscape of threats does not change significantly and the main ones are: phishing and other manifestations of social engineering, malware, ART attacks and DoS / DDoS attacks.

In order to determine the priority areas of information policy in the context of financial security, a study of the experience of leading countries. It is established that developed countries follow the path of purposeful legal regulation of relations in the national information space, adoption of necessary legislation, restructuring the activities of public authorities responsible for the implementation of information policy. Identified opportunities for implementation in Ukraine. First of all, it is the development of a national information infrastructure capable of counteracting external and internal risks and threats, ensuring the protection of national interests, including economic ones. At the same time, the effectiveness of the measures to be implemented is possible only if they are comprehensive and systematic.

Ключові слова: фінансова безпека, інформаційна політика, інформаційна безпека, ефективність, діджиталізація.

Key words: financial security, information policy, information security, efficiency, digitalization.

Постановка проблеми. В сучасних умовах зростання зовнішньої інформаційної агресії, посилення такого явища як «інформаційна війна», поширення деструктивної інформаційної пропаганди, одним з головних пріоритетів України є забезпечення формування інклюзивного та інформаційно стійкого суспільства. Враховуючи те, що інформаційні загрози чинять негативний вплив на економічні інтереси громадян, суб'єктів господарювання та держави в цілому, спричиняють значні фінансові втрати, інформаційна політика та рівень її ефективності безпосередньо впливають на забезпечення фінансової безпеки держави.

В умовах діджиталізації інформація виступає стратегічним національним ресурсом, який відіграє все більш значиму роль у системі національної безпеки. Швидкий розвиток інформаційної сфери безпосередньо впливає на політичну, економічну, соціальну та інші складові безпеки кожної держави, тому державна інформаційна політика повинна сприяти формуванню безпечного національного та світового інформаційного простору, інформаційної стійкості громадян [1].

Аналіз останніх досліджень та публікацій. Проблеми забезпечення фінансової безпеки широко актуалізуються у працях вітчизняних науковців, зокрема З. Варналія, О. Барановський, С. Онищенко, Н. Юрків та багатьох інших. Так, у дослідженнях З. Варналія обґрунтовано теоретико-методологічні засади фінансової безпеки держави, проблеми та перспективи забезпечення фінансової безпеки України за окремими її складовими, в тому числі інформаційної [2]. Праці Барановського О. присвячені методології оцінки та механізмам забезпечення фінансової безпеки України [3]. У дослідженнях Онищенко С. актуалізуються проблеми мінімізації ризиків і загроз та забезпечення складових фінансової безпеки як на рівні держави, так і

на рівні суб'єктів господарювання [4]. В працях Н. Юрків розкрито теоретико-методологічні засади і прикладні засоби підвищення рівня фінансової безпеки реального сектору економіки [5]. Водночас питання значення інформаційної політики в аспекті забезпечення фінансової безпеки держави залишається недостатньо вивченим.

Формування цілей статті. Метою дослідження є актуалізація значення інформаційної політики в умовах діджиталізації та визначення її місця в системі забезпечення фінансової безпеки держави.

Основні результати. В умовах стрімкого розвитку цифрових технологій, відсутності достатнього рівня інформаційної культури та медіаграмотності в суспільстві формується підґрунтя для маніпулювання громадською думкою, проведення стрімких деструктивних інформаційних операцій [6], що зумовлює існування потенційних та реальних загроз інформаційній, фінансовій та в цілому національній безпеці України. В цьому аспекті значення інформаційної політики як ніколи актуалізується.

Статтею 6 Закону України «Про інформацію» установлено, що державна інформаційна політика – це сукупність основних напрямів і способів діяльності держави по одержанню, використанню, поширенню та зберіганню інформації [7].

Відповідно до Закону державна інформаційна політика спрямована на забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації; формування в Україні інформаційно стійкого суспільства; розвиток та удосконалення системи електронного урядування; постійне оновлення, збагачення та зберігання національних інформаційних ресурсів тощо [8]. Враховуючи, що розвиток ІТ-технологій, цифровізація галузей національної економіки поряд з безумовно позитивним впливом на соціально-економічний стан країни створюють умови для поширення кіберзлочинів, одним із найважливіших завдань державної інформаційної політики в сучасних умовах правомірно визначити упередження й запобігання злочинам і шахрайствам у кіберпросторі та, як результат, підвищення рівня фінансової безпеки України [1].

Стрімкий розвиток комп'ютерних технологій, глобальний характер систем масової комунікації свідчать про зростання ролі інформаційної складової як для забезпечення фінансової, так і національної безпеки в цілому. Інформація стала стратегічним національним ресурсом, від рівня захищеності якої залежить захист економічних інтересів громадян, бізнесу та держави. Це підтверджує цитата Річарда Ніксона: «Один долар, вкладений в інформацію і пропаганду, значно цінніший за 10 доларів, вкладених у створення зброї, бо остання навряд чи буде вжита, в той час, як інформація працює щохвилино і повсюдно», [9] – можна впевнено стверджувати, що в сучасному світі саме інформаційна політика є головною складовою забезпечення фінансової безпеки будь якої країни та її національної безпеки в цілому.

Таким чином, доцільно розглянути систему інформаційної політики та її місце в забезпеченні фінансової безпеки (рис. 1).

Суб'єктами інформаційних відносин виступають органи державної влади, громадяни, юридичні особи, міжнародні організації. Об'єктом інформаційних відносин є інформація.

Метою державної інформаційної політики є якісне інформаційне забезпечення стратегічних і оперативних завдань соціально-економічного розвитку держави, створення інформаційно стійкого до зовнішніх та внутрішніх загроз суспільства.

Завдання, на які спрямована інформаційна політика є надзвичайно важливими. Зокрема, створення розвиненого інформаційного середовища, ефективного формування і використання національних інформаційних ресурсів, стимулювання інновацій та забезпечення всебічного розвитку й захисту національної інформаційної інфраструктури. Водночас сьогодні одним із найважливіших можна визначити уникнення ризиків (зокрема, фінансових втрат від неповної і нескоординованої експлуатації інформації, несанкціонованого використання інформації) та запобігання загрозам заподіяння в процесі інформаційної діяльності шкоди життєво важливим інтересам особи, суспільства, держави.

Рис. 1. Інформаційна політика та її місце в системі забезпечення фінансової безпеки держави

*Складено авторами

Інформаційна політика, особливо в умовах надзвичайних ситуацій, зокрема, пандемії COVID-19, є одним із основних інструментів, здатних протистояти поглибленню кризових станів, забезпечити безпеку громадян, суб'єктів господарювання та держави в цілому. Виважена інформаційна політика, забезпечуючи надання повної та достовірної інформації, в тому числі про перебіг пандемії та її наслідків, усуваючи неправдиву інформацію, дозволяє уникнути панічних настроїв населення країни.

З урахуванням постійно зростаючих реальних та потенційних ризиків і загроз в інформаційному середовищі, інформаційна політика має бути спрямована на досягнення стану захищеності систем обробки і зберігання даних, при якому забезпечується конфіденційність, доступність та цілісність інформації; створення комплексу заходів, спрямованих на забезпечення захищеності інформації суспільства і держави від

несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки запису чи знищення, тобто забезпечення інформаційної безпеки [10].

Загрози інформаційному середовищу та інформаційній безпеці можна поділити на два види: загрози, які створює сама інформація, та загрози, що створенні ззовні. У першому випадку, загроза виникає внаслідок використання інформації, яка стає знаряддям протиправних дій. У другому випадку, загроза настає від зазіхань осіб на інформацію з метою диференціювати або знищити її.

До основних загроз інформаційній безпеці, які повинні попереджатися, належать:

- 1) неповнота, невчасність та невірогідність інформації, що використовується;
- 2) негативний вплив інформації;
- 3) негативні наслідки застосування інформаційних технологій;
- 4) несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Чи не найбільшу загрозу інформації в умовах пандемії становлять фейки (що є спотворенням правди), які становлять 40% дописів про COVID-19 створеними фейковими сторінками протягом 2020 року [11].

Варто зазначити, що загрози інформаційній безпеці не можуть бути подолані лише технічними засобами, адже вони залишають поза увагою «соціальний елемент», яким є учасники відповідних відносин. Задля вирішення проблеми безпеки інформації необхідно врахувати два аспекти: законодавчу та правозастосовну.

Окрім створення актів законодавства, задля гарантування інформаційної безпеки необхідно активізувати застосування вже існуючих норм законодавства, які у багатьох випадках досить ефективно захищають права та інтереси IT-відносин, пов'язаних з інформаційною безпекою. Оскільки для забезпечення інформаційної безпеки допускається застосування певних обмежень та засобів державного примусу, виникає протиріччя права на інформацію та використання загальних засобів здійснення [12].

Забезпечення інформаційної безпеки стає гострішою, оскільки через пандемію COVID-19 значно зріс рівень діджиталізації економіки (рис. 2). В Україні кількість інтернет-користувачів у 2019 році збільшилась на 8%. Про це свідчать результати дослідження Інтернет асоціації України. Так, станом на 2019 рік всесвітньою мережею регулярно користувалися 22,96 млн українців, або 71% усього населення країни [13].

Рис. 2. Питома вага користувачів Інтернету серед дорослого населення України у 2015-2020 роках
*Побудовано авторами за [13]

У зв'язку з пандемією COVID-19 та спричиненими нею карантинними обмеженнями відбулося стрімке зростання користувачів мережі Інтернет. Згідно з підсумками дослідження, проведеними компанією GlobalLogic, за рік їх питома вага зросла на 21% і склала 92% на кінець 2020 року [14].

Порівняно із розвинутими країнами Західної Європи та Північної Америки проникнення Інтернету в Україні відбувається повільніше. Експерти вважають, що протягом наступних трьох років порівняно з до пандемічним періодом (2019 роком) темп росту цифровізації економіки зросте на 1-5%. Від впливу цифровізації найбільше вииграє сектор комп'ютерного програмування, поштова та кур'єрська служба, телекомунікація та освіта [15, 16].

Разом із зростанням рівня діджиталізації зростають і загрози безпеці інформації, а саме кіберзагрози. Саме цей вид загроз інформаційній безпеці спричиняє найбільші фінансові втрати і, безперечно, впливають на рівень фінансової безпеки країни в цілому. Кіберзлочинці найчастіше атакують користувачів Інтернетом через месенджери. У 2021 році 45% з опитаних українців стикалися зі спробами онлайн-шахрайства. У 2020 році цей показник становив 22%. Найбільше з початку 2021 року кібератак зазнали мешканці великих міст. Згідно з офіційними статистичними даними рівень кіберзлочинності в Україні постійно зростає (рис. 3).

Рис. 3. Рівень та динаміка кіберзлочинів в Україні у 2010 – 2020 рр.

*Побудовано авторами за [17]

Слід відмітити, що Україна лідирує за кількістю кібератак у світових рейтингах, що свідчить про низький рівень захисту інформаційного середовища.

Розглядаючи структуру кіберзлочинів у 2020 році, встановлено, що найбільшу частку (54%) шахрайських випадків становив продаж неіснуючих товарів на умовах попередньої оплати. 28% у структурі кіберзлочинів склали фішингові атаки, коли у повідомленнях користувачам надсилалися шкідливі посилання на підроблену платіжну форму з метою викрадення особистих даних користувача. 11% становили шахрайства, пов'язані з надсиланням фейкових скріншотів / квитанцій про оплату за товару (рис. 4).

Основною причиною успішності кібератак є саме людський фактор – 91% зломів здійснюються в результаті вдалого фішингу.

Рис. 4. Структура кіберзлочинів в Україні у 2020 році

*Побудовано авторами за [16]

Згідно з опитуванням Harvey Nash/KPMG CIO Survey 4 з 10 IT-лідерів повідомляють, про зростання кібератак, понад три чверті цих атак відбулися через фішинг (83%) і майже дві третини через шкідливе програмне забезпечення (62%), що доводить те, що масовий перехід на роботу онлайн збільшив ризик і незахищеність роботи працівників [18].

Так, згідно з офіційними даними розробника програмного забезпечення в сфері захисту інформації та кібербезпеки ESET, за 2020 рік в Україні у два рази збільшилась кількість веб-загроз і кібератак, в тому числі через електронну пошту (шкідливе програмне забезпечення, програми-вимагачі сімейства WannaCryptor, завантажувачі та криптомайнери, експлойти EternalBlue і т.ін.). Водночас фінансові втрати світової економіки

через кіберзлочини у 2020 році перевищили 1 трлн. доларів, що більше майже вдвічі у порівнянні з 2018 роком [19].

Ці дані підтверджують значення інформаційної політики, як основної складової інформаційної безпеки, для забезпечення фінансової безпеки держави.

Таким чином, стрімкий розвиток інформаційних технологій ставить нові виклики не лише перед Україною, а в цілому перед світовою спільнотою. Сьогодні розвинуті країни прямують шляхом цілеспрямованого правового впорядкування відносин у національному інформаційному просторі, приймання необхідних законодавчих актів, перебудовуючи діяльність органів державної влади, які відповідають за реалізацію інформаційної політики.

Для прикладу, Великобританія, маючи за мету вдосконалення умов конкуренції на інформаційному ринку та підвищення ефективності інформаційних послуг, реалізує інформаційну політику на принципах технологічної нейтральності законів, сприянню міжнародному співробітництву, захисту інтересів споживача в комп'ютерних системах і мережах.

Німеччина має на меті безперешкодний транскордонний обмін інформацією, розвиток цифрових технологій, вільну конкуренцію в інформаційній сфері.

Тим часом уряд Франції створив Фонд допомоги і співробітництва для підтримки впровадження вітчизняних інформаційних технологій, задля стимулювання наукових досліджень у галузі ІТ-технологій, створення систем безпеки інформації та запобігання комп'ютерним злочинам.

В основу чинної інформаційної політики Європейського Союзу покладено доктрину європейського інформаційного суспільства, основна ідея якої полягає у перенесенні акцентів з геополітики на технополітику, що реалізується у рамках компетенції міжнародних регіональних організацій, які вирішують весь комплекс політичних, економічних і соціальних проблем європейських країн [20]. Нормативно-правова база ЄС в інформаційній сфері постійно доповнюється та розширюються, в наслідок чого є дуже широкою та розгалуженою.

Інформаційна політика США спрямована на підтримку наукових досліджень і розробок у сфері інформації і телекомунікації, на сприяння обміну технологіями між університетами та фірмами, створення і удосконалення інформаційної інфраструктури, забезпечення збалансованості між основними інформаційними цінностями.

США жорстко контролюють питання щодо державної таємниці, яка знаходиться в урядових і комерційних телекомунікаційних мережах, що унеможлиблює її витік за межі країни. Конгресом США у 1987 р. був прийнятий Закон «Про забезпечення безпеки ЕОМ», який встановив пріоритет національних інтересів при вирішенні питань безпеки інформації, зокрема приватної [21].

Слід зазначити, що аналіз дослідження наукових розвідок щодо інформаційної безпеки США показав, що, не зважаючи на велику кількість нормативно-правових актів в сфері інформаційної безпеки, вони не завжди були ефективними, адже законодавство США не охоплювало всіх загроз в інформаційній сфері держави, особливо після 11 вересня 2001 р. (дата, відома як теракт у Лос-Анжелесі з наймасштабнішими наслідками). Тому захист інформаційного простору від кібертерористів та шахрайства сприяли розробці нормативно-правових актів з інформаційної безпеки США принципово нового, більш високого рівня.

В цілому за останні 35 років у США сформувалася чітка, досконала система забезпечення інформаційної безпеки, яка характеризується поступовими тенденціями та кардинальними заходами. Тому американський досвід державної політики в сфері інформаційної безпеки є важливим для української зовнішньої та внутрішньої політики, а особливо, найціннішим є дієвий підхід до регулювання ринку інформаційних технологій та забезпечення фінансової безпеки країни.

Важливо звернути увагу, що в умовах інформаційної агресії для України американський досвід використання інформаційних технологій для створення систем зв'язку та військового управління є надзвичайно важливим.

Прийняття у 2021 році Стратегії інформаційної безпеки України стало важливим кроком в напрямку підвищення ефективності інформаційної політики. Водночас, з урахуванням позитивного світового досвіду, правомірно виділити наступні напрями реалізації інформаційної політики в аспекті забезпечення фінансової безпеки України.

1. Розвиток національної інформаційної інфраструктури, здатної протидіяти зовнішнім та внутрішнім ризикам і загрозам, забезпечувати захист національних інтересів, зокрема економічних.
2. Зміцнення інституційної спроможності у сфері стратегічних комунікацій, що передбачає формування механізму координації та взаємодії між органами державної влади, які реалізують заходи протидії ризикам і загрозам в інформаційній, фінансовій та інших сферах національної економіки.
3. Підвищення рівня інформаційної спроможності населення, а саме забезпечення вільного доступу до об'єктивної, неупередженої та правдивої інформації.
4. Забезпечення зростання рівня інформаційної культури й медіаграмотності в суспільстві як базису для протидії деструктивним інформаційним впливам.

Державна інформаційна політика в умовах глобалізації буде ефективною лише у тому разі, якщо вона матиме комплексний, системний характер і, безперечно, буде відкритою, наведеною на забезпечення економічних інтересів громадян, бізнесу і держави.

Висновки. Інформаційна політика країни має велике значення, адже від її ефективності залежить запобігання шкоди національним інтересам, запобігання шкідливій зміні свідомості і поведінки людей, забезпечення фінансової безпеки України та національної безпеки в цілому. Державна інформаційна політика має забезпечувати свободу інформації, сприяти розвитку нових інформаційно-комунікаційних технологій, створювати більш відкрите управління суспільними програмами. Проведення інформаційної політики має ґрунтуватися на реалізації комплексу заходів, спрямованих на розвиток інформаційного середовища, стійкого до зовнішніх і внутрішніх ризиків та загроз, що посилюються в умовах діджиталізації.

Література.

1. Глушко А.Д., Пантась В.В., Бабенко С.Р. Інституційно-правове забезпечення інформаційної політики України. «*EURASIAN SCIENTIFIC DISCUSSIONS*»: матеріали I Міжнародної науково-практичної конференції, 13 лютого 2022 р., Барселона, Іспанія. С. 511–514.
2. Варналій З.С. Економічна та фінансова безпека України в умовах глобалізації : монографія. Київ : Знання України, 2020. 423 с.
3. Барановський О.І. Фінансова безпека в Україні (методологія оцінки та механізми забезпечення). Київ : КНТЕУ, 2004. 760 с.
4. Онищенко С.В., Варналій З.С. Сучасні тенденції структурних складових фінансової безпеки України в умовах глобальних перетворень. *Формування ринкової економіки в Україні*, 2016. Т. 35. С. 75-80.
5. Юрків Н.Я. Економічна безпека реального сектора економіки України: стратегічні пріоритети і теоретико-методологічні засади забезпечення: монографія. Львів : ПАІС, 2012. 400 с.
6. Стратегія інформаційної безпеки (затверджена Указом Президента України від 28 грудня 2021 року). URL: <https://www.president.gov.ua/documents/6852021-41069>
7. Правове забезпечення державної інформаційної політики. Міністерство юстиції України. URL: <https://minjust.gov.ua/m/str/22116>
8. Закон України «Про інформацію». Редакція від 01.01.2022 р. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
9. Печенюк А.В. Інформаційна безпека України як складова національної безпеки. URL: <https://www.ndifp.com/1561/>
10. Закон України «Про захист інформації в інформаційно-комунікаційних системах». Редакція від 01.01.2022. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>
11. Харитонов Є.О. COVID-19 та проблеми інформаційної безпеки. URL: <http://dspace.onua.edu.ua/bitstream/handle/>
12. Аудит інформаційної безпеки: підручник / В.А. Ромака, А.Е. Лагун, Ю.Р. Гарасим та ін.; Держ. служба України з надзвич. ситуацій, Львів. держ. ун-т безпеки життєдіяльності, НАН України, Ін-т приклад. проблем механіки і математики ім. Я.С. Підстригача. Львів: Сполом, 2015. 363 с.
13. Інтернет Асоціація України. URL: <http://watcher.com.ua/2017/04/13/bilshe-polovyny-zhyteliv-sil-v-ukrayini-vzhe-korystuyutsya-internetom/>
14. Дослідницький холдинг Factum Group Ukraine. URL: <https://mind.ua/news/20204323-majzhe-23-mln-ukrayinciv-regulyarno-koristuyutsya-internetom-doslidzhennya>
15. Вплив COVID-19 на економіку і суспільство країни: консенсус-прогноз. URL: <https://www.me.gov.ua/Documents/List?lang=uk-UA&tag=Konsensus-prognoz&pageNumber=1>
16. Онищенко С.В., Глушко А.Д. Концептуальні засади інформаційної безпеки національної економіки в умовах діджиталізації. *Соціальна економіка*. ХНУ, 2020. Вип. 59. с. 14–24. URL: <https://periodicals.karazin.ua/socoeconom/article/view/16114>
17. Дані Департаменту кіберполіції України: офіційний сайт URL : <https://cyberpolice.gov.ua/results/2018/>
18. Офіційний сайт KPMG. URL: <https://home.kpmg/ua/uk/home.html>
19. The Hidden Costs of Cybercrime. URL: <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf>
20. Мохова Ю.Л., Луцька А.І. Сутність та головні напрямки державної інформаційної політики України. URL: http://www.dy.nayka.com.ua/pdf/12_2018/27.pdf
21. Центр досліджень соціальних комунікацій НБУВ. Інформаційна безпека США: законодавче регулювання та перспективи співпраці для України. URL: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2988:informatsijna-bezpeka-ssha-zakonodavche-regulyuvannya-ta-perspektivi-spiivpratsi-dlya-ukrajini&catid=8&Itemid=350

References.

1. Hlushko, A.D., Pantas V.V. and Babenko S.R. (2022), “Institutional and legal support of information policy of Ukraine”, *EURASIAN SCIENTIFIC DISCUSSIONS*, Barcelona, Spain, 13 February, Pp. 511–514.
2. Varnalii, Z.S. (2020), *Ekonomichna ta finansova bezpeka Ukrainy v umovakh hlobalizatsii* [Economic and financial security of Ukraine in the context of globalization], Znannia Ukrainy, Kyiv, Ukraine.

3. Baranovskii, O.I. (2004), *Finansova bezpeka v Ukraini (metodolohiia otsinky ta mekhanizmy zabezpechennia)* [Financial security in Ukraine (evaluation methodology and support mechanisms)], KNTEU, Kyiv, Ukraine.
4. Onyschenko, S.V., Varnalii, Z.S. (2016), "Current trends in the structural components of Ukraine's financial security in the context of global transformation", *Formuvannia rynkovoi ekonomiky v Ukrainy*, vol. 35, no. 1, pp. 75–80.
5. Yurkiv, N.Ya. (2012), *Ekonomichna bezpeka real'noho sektora ekonomiky Ukrainy: stratehichni priorytety i teoretyko-metodolohichni zasady zabezpechennia* [Economic security of the real sector of Ukraine's economy: strategic priorities and theoretical and methodological principles of ensuring], PAIS, Lviv, Ukraine.
6. President of Ukraine (2021), "Information security strategy", available at: <https://www.president.gov.ua/documents/6852021-41069> (Accessed 16 Feb 2022).
7. Ministry of Justice of Ukraine (2021), "Legal support of the state information policy", available at: https://minjust.gov.ua/m/str_22116 (Accessed 10 Feb 2022).
8. The Verkhovna Rada of Ukraine (1992), The Law of Ukraine "About information", available at: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> (Accessed 10 Feb 2022).
9. Pechenyuk, A.V. (2020), "Information security of Ukraine as a component of national security", [Online], available at: <https://www.ndifp.com/1561/> (Accessed 16 Feb 2022).
10. The Verkhovna Rada of Ukraine (1994), The Law of Ukraine "On information protection in information and communication systems", available at: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text> (Accessed 16 Feb 2022).
11. Harytonov, Ye.O. (2021), "COVID-19 and information security issues", [Online], available at: <http://dspace.onua.edu.ua/bitstream/handle/> (Accessed 16 Feb 2022).
12. Romaka, V.A., Lagun, A.E. and Harasem, A.R. (2015), *Audyt informatsijnoi bezpeky* [Information security audit], Spolom, Lviv, Ukraine.
13. Internet Association of Ukraine (2022), available at: <http://watcher.com.ua/2017/04/13/bilshe-polovyny-zhyteliv-sil-v-ukrayini-vzhe-korystuyutsya-internetom/> (Accessed 16 Feb 2022).
14. Mind (2019), "Research holding Factum Group Ukraine", available at: <https://mind.ua/news/20204323-majzhe-23-mln-ukrayinciv-regulyarno-koristuyutsya-internetom-doslidzhennya> (Accessed 16 Feb 2022).
15. Ministry of Economy of Ukraine (2022), "Impact of COVID-19 on the country's economy and society: consensus forecast", available at: <https://www.me.gov.ua/Documents/List?lang=uk-UA&tag=Konsensus-prognoz&pageNumber=1> (Accessed 16 Feb 2022).
16. Onyschenko, S.V. and Hlushko, A.D. (2020), "Conceptual principles of information security of the national economy in the conditions of digitalization", *Sotsial'na ekonomika*, HNU, vol. 59, pp. 14–24, available at: <https://periodicals.karazin.ua/soceconom/article/view/16114> (Accessed 17 Feb 2022).
17. Cyberpolice Department of Ukraine (2022), available at: <https://cyberpolice.gov.ua/results/2018/> (Accessed 11 Feb 2022).
18. KPMG (2022), available at: <https://home.kpmg/ua/uk/home.html> (Accessed 11 Feb 2022).
19. McAfee (2020), "The Hidden Costs of Cybercrime", available at: <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf> (Accessed 11 Feb 2022).
20. Mohova, Yu.L. and Lutska, A.I. (2018), "The essence and main directions of the state information policy of Ukraine", *Derzhavne upravlinnia: udoskonalennia ta rozvytok*, [Online], vol. 12, available at: http://www.dy.nayka.com.ua/pdf/12_2018/27.pdf (Accessed 16 Feb 2022).
21. Center for Social Communications Research NBUV (2022), "US Information Security: Legislation and Prospects for Cooperation for Ukraine", available at: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2988:informatsijna-bezpeka-ssha-zakonodavche-regulyuvannya-ta-perspektivi-spivpratsi-dlya-ukrajini&catid=8&Itemid=350 (Accessed 16 Feb 2022).

Стаття надійшла до редакції 18.02.2022 р.