

DOI: [10.32702/2307-2156-2019.11.3](https://doi.org/10.32702/2307-2156-2019.11.3)

УДК 004.738.5:34:35

*О. А. Панченко,  
директор ДЗ «Науково-практичний медичний реабілітаційно-діагностичний центр МОЗ України»,  
Заслужений лікар України, доктор медичних наук, професор,  
президент Всеукраїнської професійної психіатричної ліги (м. Київ),  
ORCID: 0000-0001-9673-6685*

## **ПРОБЛЕМИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ**

*О. А. Panchenko  
Director of the State Institution "Scientific – Practical Medical  
Rehabilitating – Diagnostic Center of the Ukrainian Ministry of Health",  
Honored Doctor of Ukraine, Doctor of Medicine, Professor,  
President of the All-Ukrainian Professional Psychiatric League, Kyiv*

### **PROBLEMS OF LEGAL SUPPORT OF THE PUBLIC ADMINISTRATION OF THE INFORMATION SECURITY**

*У статті проаналізовано проблеми правового забезпечення державного управління інформаційною безпекою України. В Україні, як і в багатьох державах світу, проблеми правового забезпечення системи безпеки, суспільства й особистості стають дедалі актуальнішими у національній політиці та державному управлінні.*

*Сформульоване наступне визначення поняття інформаційна безпека - це стан інформаційного середовища, що забезпечує задоволення інформаційних потреб суб'єктів інформаційних відносин, безпеку інформації та захист суб'єктів від негативного інформаційного впливу. В даному визначенні суб'єктами інформаційних відносин можуть бути: держава, суспільство, організації, людина. Чинне законодавство України не містить відповідного розгорнутого тлумачення поняття «інформаційна безпека держави», проте нормативні акти, які торкаються питань інформаційної безпеки, закономірно розглядають її в контексті більш загального поняття національної безпеки.*

*Рівень інформаційної безпеки активно впливає на стан політичної, економічної, оборонної та інших складових національної безпеки України, бо найчастіше реалізація інформаційних загроз – це завдання шкоди в політичній, військовій, економічній, соціальній, екологічній сферах тощо. До нормативно-правової бази належать керівні документи державної політики, що створюють основу стратегічного планування: закон, доктрина, концепція, стратегія, що регламентують суспільні відносини у сфері національної безпеки. Але, на жаль, нині в Україні немає реальних гарантів її інформаційної безпеки, відсутній комплекс нормативно-правових актів щодо захисту інформаційних ресурсів та інформаційної інфраструктури.*

*Для реалізації національних інтересів в інформаційній сфері слід переглянути пріоритети державної політики, розробити нові концептуальні підходи щодо регулювання ринку*

*інформаційно-комунікаційних технологій, інформаційної та інвестиційної політики, розвитку інформаційного законодавства та забезпечення інформаційної безпеки.*

*In the article the problems of legal security of the public administration of the Ukraine's information security were analysed. In Ukraine, as in many countries of the world, the problems of legal support of the security system of the state, society and the individual are becoming increasingly relevant in public policy and public administration.*

*The following definition of the concept of information security is formulated: it is the state of the information environment that ensures the satisfaction of the information needs of the subjects of information relations, information security and the protection of subjects from negative information impact. In this definition, the subjects of information relations can be: the state, society, organizations, people. The current legislation of Ukraine does not contain a corresponding expanded interpretation of the concept of "information security of the state", however, normative acts regarding information security issues naturally consider it in the context of a more general concept of national security.*

*The level of information security actively affects the state of the political, economic, defense and other components of the national security of Ukraine, because most often the implementation of information threats is harm in the political, military, economic, social, environmental spheres etc. The legal frameworks includes the governing documents of state policy, which form the basis of strategic planning: the law, doctrine, concept, strategy, which regulate public relations in the field of national security. But, unfortunately, now in Ukraine there are no real guarantors of its information security, there is no set of legal acts to protect information resources and information infrastructure.*

*To realize national interests in the information sphere, it is necessary to revise the priorities of state policy, develop new conceptual approaches to regulate the market of information and communication technologies, information and investment policies, develop information legislation and ensure information security.*

**Ключові слова:** *інформаційна безпека; національна безпека; інформаційна безпека держави; державне управління; загрози та ризики.*

**Key words:** *information security; national security; public administration; information security of the state; threats and risks.*

## **1. ВСТУП**

**Постановка проблеми.** В Україні, як і в багатьох державах світу, проблеми правового забезпечення системи безпеки держави, суспільства й особистості стають дедалі актуальнішими у державній політиці та державному управлінні. У змістовному плані інформаційна безпека є складовою частиною національної безпеки та займає особливе місце у її структурі. Це обумовлено тим, що без інформаційного забезпечення всі види безпеки не можуть бути реалізовані в повному обсязі.

Інформаційна безпека належить до числа пріоритетних цілей сучасної держави та є одним з головних факторів його стабільного розвитку. Зрозуміло, що системні збої у функціонуванні механізмів забезпечення інформаційної безпеки можуть привести до економічних, соціально-політичних, і техногенних зрушень, що здатні підірвати можливість органів державного управління належним чином здійснювати свої основні функції. Саме тому на сучасному етапі розвитку України надзвичайно актуальним є розв'язання проблеми державного управління у сфері інформаційної безпеки.

В умовах формування інформаційного суспільства інформація являє собою один із вирішальних ресурсів розвитку цивілізації, активно впливає на всі сфери життя, формує нові уявлення про працю і знання. За умов глобалізації інформаційних ресурсів відбуваються інтеграція інформаційних систем різних держав до єдиної загальної світової інформаційної системи, формування єдиного інформаційного простору, створення глобальних інформаційно-телекомунікаційних мереж, інтенсивне впровадження нових інформаційних технологій в усі галузі суспільного життя.

Однак, доступність інформації, широке різноманіття джерел її отримання, наповнення внутрішньодержавного та світового інформаційного простору, на поверхні позитивних процесів, можуть нести

не тільки благо, але і шкоду інтересам особи, суспільства і держави, безпосередньо загрожуючи національній безпеці.

У зв'язку з цим надзвичайну вагомість набувають питання визначення правового забезпечення інформаційної безпеки як однієї з найважливіших складових національної безпеки, що впливає на прийняття державою тактичних та стратегічних рішень.

Вибрана тема дослідження покликана сприяти вирішенню означеної проблеми.

#### **Аналіз останніх досліджень і публікацій.**

Питання державного управління у сфері безпеки (національної, регіональної тощо), її забезпечення організаційними, інформаційними та іншими методами досліджували О. Власенко, В. Гурковський, Л. Євдоченко, З. Коваль, Г. Головка, С. Домбровська, В. Косевцова, Ю. Машкарова, Н. Нижник, А. Помази-Пономаренко, В. Стрельцова та ін. Проблеми, що існують у цій сфері, аналізують багато українських та закордонних вчених, такі як В. Богданович, О. Астахов, М. Єрмошин, А. Семенченко, С. Мосов, В. Горбулін, І. Романченко та ін.

Проте залишається актуальною потреба у смисловому наповненні самого поняття «інформаційна безпека» з державної точки зору, визначення політики захисту національного інформаційного простору, вдосконалення правового забезпечення державного управління інформаційною безпекою.

**Метою дослідження** є визначення проблем правового забезпечення державного управління інформаційною безпекою та шляхів їх вирішення.

## **2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ**

У найбільш широкому визначенні безпека являє собою стан захищеності від чого завгодно та може застосовуватися як щодо особистості зокрема, так і суспільства та держави в цілому. Разом з тим, безпека як поняття, відрізняється в залежності від сфери застосування: політології, соціології економіки і т.д. Так, в теорії національної безпеки широко використовуються такі формулювання: «національна безпека», «безпека особистості», «державна безпека», «міжнародна безпека», «інформаційна безпека», «політична безпека», «соціальна безпека», «військова безпека» та ін. [15].

Сьогодні з поняттям «інформаційна безпека», зокрема, з його термінологічним визначенням, склалася парадоксальна ситуація. З одного боку, термін «інформаційна безпека» широко використовується в наукових публікаціях, навчальній літературі та законодавчих документах різного рівня, з іншого боку, це поняття досі не має однозначного розуміння, а його зміст у різних джерелах має кардинальні розбіжності [8].

Як показує аналіз наукової літератури стосовно питання інформаційної безпеки, більшість науковців сходяться на думці, що інформаційна безпека – це складова частина національної безпеки, що становить собою: 1) стан захищеності життєво-важливих інтересів особи, суспільства і держави, за якого зводиться до мінімуму нанесення шкоди через неповність, несвоєчасність та недостовірність інформації; деструктивний її вплив; несанкціоноване поширення. 2) стан захищеності національного інформаційного простору, який забезпечує формування, використання і розвиток останнього в інтересах громадян, організацій, держави [8].

У цілому змістове наповнення поняття «інформаційна безпека» визначається трьома складовими [12]:

*Перша* – задоволення інформаційних потреб суб'єктів в інформаційному середовищі. Очевидно, що без наявності у суб'єкта необхідної інформації не може бути забезпечена інформаційна безпека. Інформаційні потреби різних суб'єктів не однакові, однак в будь-якому випадку відсутність необхідної інформації може мати негативні наслідки.

*Друга* – безпека інформації. Вимоги повноти, достовірності та своєчасності інформації повинні дотримуватися протягом усього часу циркуляції інформації, оскільки їх порушення може призвести до невірних рішень або взагалі до неможливості прийняття рішень, як і порушення статусу конфіденційності може знецінити інформацію. Тому інформація повинна бути захищена від впливів, що порушують її статус.

*Третя* – захист суб'єктів інформаційних відносин від негативного інформаційного впливу. До прийняття невірних рішень може привести не тільки відсутність необхідної інформації, але і наявність шкідливої, небезпечної для суб'єкта інформації, яка найчастіше цілеспрямовано нав'язується.

При такому підході можна сформулювати наступне визначення: *Інформаційна безпека – стан інформаційного середовища, який забезпечує задоволення інформаційних потреб суб'єктів інформаційних відносин, безпеку інформації та захист суб'єктів від негативного інформаційного впливу.* В даному визначенні суб'єктами інформаційних відносин можуть бути: держава, суспільство, організація, людина.

У контексті національної безпеки, інформаційна безпека може розглядатися, з одного боку, як самостійний її елемент, а з іншого – як інтегрована складова будь-якої іншої безпеки: військової, економічної, політичної і т.д. У такому руслі більш повним визначенням інформаційної безпеки можна вважати наступне: *«інформаційна безпека – це стан захищеності життєво важливих інтересів особистості, суспільства і держави, при якому зводиться до мінімуму завдання шкоди через неповноту, невчасність та невірність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації»* [9, 13].

Чинне законодавство України не містить відповідного розгорнутого тлумачення поняття «інформаційна безпека держави», проте нормативні акти, які торкаються питань інформаційної безпеки, закономірно розглядають її в контексті більш загального поняття національної безпеки. Такий підхід значно обмежує та звужує зміст категорії «інформаційна безпека держави», позаяк виключно інформаційний простір

слугує каналом реалізації загроз національній безпеці в усіх сферах діяльності держави. Термін інформаційної безпеки закріплено лише у Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» [3].

Як зазначено у Законі України «Про національну безпеку» державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо [2].

Однак, національний інформаційний простір України, на превеликий жаль, зазнає суттєвих загроз, викликів, що становлять небезпеку функціонування держав, її політичного та економічного розвитку, інтеграції у європейські та євроатлантичні структури [9].

У Доктрині інформаційної безпеки України визначено, що до національних інтересів України в інформаційній сфері віднесено такі життєво-важливі інтереси особи, як забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; забезпечення конституційних прав людини на захист приватного життя; захищеність від руйнівних інформаційно-психологічних впливів. Також в ній зазначено такі загрози інформаційній безпеці країни: поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України; зовнішні деструктивні інформаційні впливи на суспільну свідомість через ЗМІ та мережу Інтернет; деструктивні інформаційні впливи, що спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності та недоторканності України; прояви сепаратизму в ЗМІ, та у мережі Інтернет за етнічною, мовною, релігійною та іншими ознаками [4].

Однак, цей документ являє собою сукупність теоретичних понять про цілі, принципи та правові складові інформаційної безпеки. Відтак, з нього не зрозуміло чітких завдань та відповідальних суб'єктів за інформаційну безпеку, оскільки він є лише основою для розроблення проектів, концепцій, стратегій, цільових програм і планів дій із забезпечення інформаційної безпеки України.

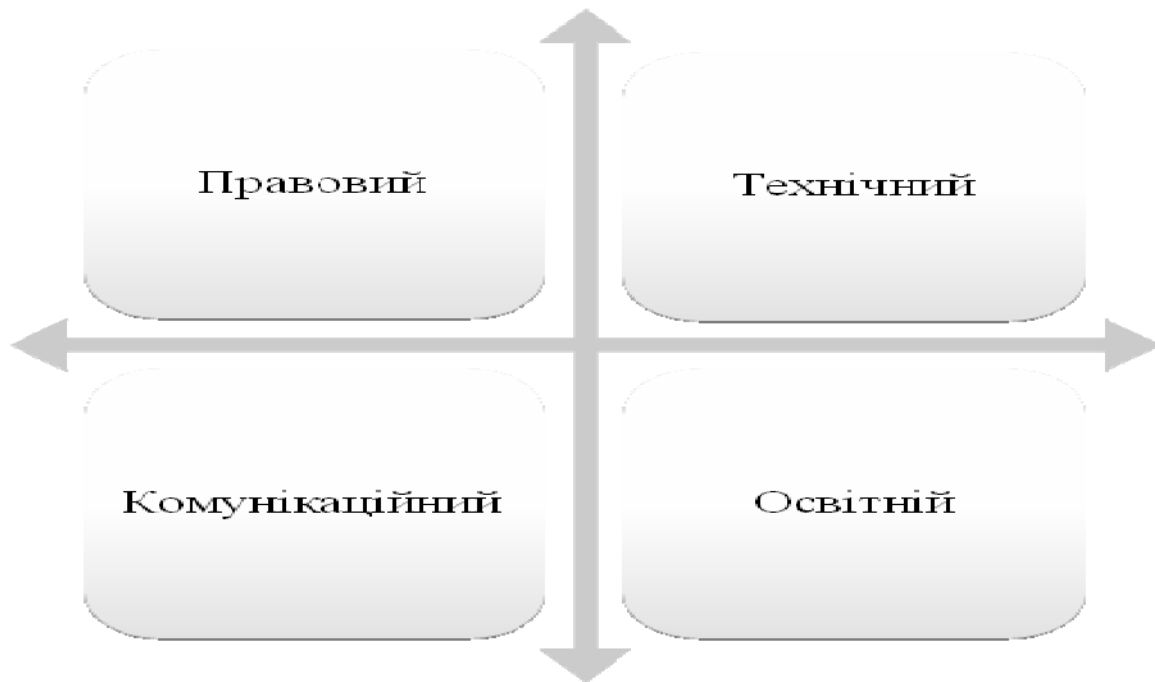
Інформаційна безпека України – передбачений Конституцією захист політичних, державних, громадських інтересів країни, загальнолюдських і національних цінностей [14]. Важливість забезпечення інформаційної безпеки задекларована в ст.17 Конституції України [1] як одна із найважливіших функцій держави та справою всього Українського народу, наряду зі захистом суверенітету, територіальної цілісності України та економічною безпекою.

У сучасних умовах найважливішим елементом інформаційної безпеки є кібербезпека. Про пріоритетність забезпечення кібербезпеки в Україні свідчить запроваджена у 2016 році Стратегія кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 року № 96/2016 [5]. Отже, початок регулюванню інформаційної безпеки в Україні покладено, що однозначно є позитивним кроком. Однак, шляхи реалізації прийнятих норм на практиці розробляються дуже повільно та у більшості випадків не слугують правовим інструментом для практичного застосування та забезпечення ефективності заходів кібербезпеки.

Основною метою державного управління є розробка та реалізація концептуальних основ державної інформаційної політики шляхом прийняття адекватних нормативно-правових актів щодо регулювання інформаційних відносин [10]. У останній час значно зросла необхідність в комплексному та ефективному підході до процесу забезпечення безпеки національного інформаційного простору, що наглядно представляється у нормативних документах закордонних країн. У провідних країнах світу протягом десятиліть створювалося законодавство з інформаційної політики та інформаційної безпеки, та як засвідчує їх досвід, великого значення для нормального функціонування інформаційної сфери держави набуває узгоджена діяльність відповідного державно-правового механізму, тобто система взаємопов'язаних державних органів, організацій, установ щодо вироблення та реалізації сукупності норм та принципів права, які повинні врегулювати суспільні відносини в інформаційній сфері [10, 11].

Прикладом, у Молдові діє Стратегія інформаційної безпеки що містить опис безпечних та правових проблем, цілі, задачі, ключові показники ефективності (KPI), план реалізації зі чітким розподілом відповідальних суб'єктів. У Данії теж на державному рівні розроблено стратегію інформаційної та кібербезпеки, що комплексно охоплює питання реалізації – від найвищого державного рівня – до безпеки людини в мережі. В Естонії, яка вважається європейським лідером із застосування цифрових технологій в економіці та адмініструванні, дбають про інформаційний захист з 1996 року.

Ураховуючи досвід найкращих світових практик, інформаційну безпеку в Україні можна розглядати як систему, що складається з чотирьох ґрунтовних компонентів (рис.1).



**Рис. 1. Компоненти системи інформаційної безпеки в Україні**

*Правовий компонент* повинен встановити норми та гарантувати юридичні механізми системи захисту інформації в державі, забезпечувати відповідний механізм попередження, реагування та розслідування будь-яких посягань на інформаційну безпеку.

*Технічний компонент* має забезпечити інженерно-технічними заходами конфіденційність, цілісність та доступність інформації.

*Комунікаційний компонент* – забезпечення системи моніторингу та формування контенту у соціальних мережах.

*Освітній компонент* – інтегроване систематичне навчання інформаційній безпеці у закладах освіти, а також підвищення кваліфікації для працівників органів державної влади та місцевого самоврядування, які працюють з інформацією [6].

Для реалізації національних інтересів в інформаційній сфері слід переглянути пріоритети державної політики, розробити нові концептуальні підходи щодо регулювання ринку інформаційно-комунікаційних технологій, інформаційної та інвестиційної політики, розвитку інформаційного законодавства та забезпечення інформаційної безпеки [7]. Враховуюче вищесказане, можна запропонувати необхідні перші кроки для посилення інформаційної безпеки (рис.2):



**Рис.2. Ключові кроки модернізації інформаційної безпеки**

1. Виявити специфічні сегменти, що вимагають реформування у сфері інформаційної безпеки, для цього провести комплексні аудити (правовий, технічний, комунікаційний та освітній) у сфері інформаційної безпеки у державних органах із залученням зацікавлених суб'єктів.

2. Сформуванню національну стратегію інформаційної безпеки та реалістичний план її виконання на основі виявлених уразливостей разом з фахівцями у сфері інформаційної безпеки.

3. Розпочати реалізацію реформи інформаційної безпеки [6].

### 3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Рівень інформаційної безпеки активно впливає на стан політичної, економічної, оборонної та інших складових національної безпеки України, бо найчастіше реалізація інформаційних загроз – це завдання шкоди в політичній, військовій, економічній, соціальній, екологічній сферах тощо. На жаль, нині в Україні немає реальних гарантів її інформаційної безпеки, відсутній комплекс нормативно-правових актів щодо захисту інформаційних ресурсів та інформаційної інфраструктури. Поряд з цим, процес інформатизації має стихійну, некеровану природу з переважним ухилом у бік використання засобів інформатизації іноземного виробництва.

Запропоновані автором заходи є лише першими необхідними кроками в посиленні державного управління інформаційною безпекою. Потрібні подальші всебічні дослідження в цьому напрямку, пріоритетами повинні стати аналіз загроз в національному інформаційному просторі та питання забезпечення інформаційної безпеки держави як частини глобального інформаційного співтовариства.

#### Список використаних джерел.

1. Конституція України від 28 червня 1996 р. *Відомості Верховної Ради України*. 1996. № 30. Ст. 17.
2. Закон України «Про національну безпеку України». *Відомості Верховної Ради України*. 2018, № 31, ст. 241.
3. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки». *Відомості Верховної Ради України* 2007, № 12, ст.102.
4. Доктрина інформаційної безпеки України, затверджена Указом президента України від 25.02.2017 р. № 47/2017. URL: <http://president.gov.ua>.
5. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України": Указ Президента України від 15.03.2016 р. № 96/2016. URL: <https://zakon.rada.gov.ua/laws/show/96/2016#n11>.
6. Апетик А. Інформаційна безпека. (2019). URL: [https://webcache.googleusercontent.com/search?q=cache:nY\\_Tl2\\_Dяп-8J:https://www.prostir.ua/%3Flibrary%3Dinformatsijna-bezpeka-now-yakyh-elementiv-ne-vystachaje+&cd=3&hl=ru&ct=clnk&gl=ua](https://webcache.googleusercontent.com/search?q=cache:nY_Tl2_Dяп-8J:https://www.prostir.ua/%3Flibrary%3Dinformatsijna-bezpeka-now-yakyh-elementiv-ne-vystachaje+&cd=3&hl=ru&ct=clnk&gl=ua).
7. Богуш В.М., Юдін О.К. Інформаційна безпека держави К.: МК-Прес, 2005. 432 с.
8. Захаренко К. Основні суб'єкти та інститути інформаційної безпеки. Науковий вісник. Серія «Філософія». Харків: ХНПУ. 2017. Вип.48 (частина I). С. 212–219.
9. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. Політичні науки. Вип. 2. № 1. 2016. С. 27–32.
10. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. К.: КНТ, 2006. 280 с. (Серія: Національна і міжнародна безпека).
11. Малик Я.Й., Береза О.І. Забезпечення інформаційної безпеки України у контексті світового досвіду. *Ефективність державного управління*. 2012. Вип. 32. С.20–27.
12. Олійник О.В. Адміністративно-правові засади інформаційної безпеки. *Європейські перспективи*. 2012. № 4(1). С. 65–68.
13. Панченко О.А. Информационная безопасность личности: монография / О.А. Панченко, Н.В. Банчук. К.: КИТ, 2011. 672 с.
14. Присяжнюк М., Белошевич Я. Інформаційна безпека України в сучасних умовах. *Вісник Київського національного університету ім. Т. Шевченка. Військово-спеціальні науки*. 2013. Вип. 30. С.29–33.
15. Форос Г.В., Жогов В.С. Особливості трактування поняття «кібербезпека» в сучасній юридичній науці. *Правова держава*. 2019. №33. С. 128–134.

#### References.

1. Constitution of Ukraine: dated June 28, 1996 (1996). *Vidomosti Verkhovnoi Rady Ukrainy*, N 30. P. 17 [in Ukrainian].
2. The Verhovna Rada of Ukraine (2018), The Law of Ukraine “On the national security of Ukraine”, *Vidomosti Verkhovnoi Rady Ukrainy*, N 31. P. 241.
3. The Verhovna Rada of Ukraine (2007), The Law of Ukraine “On the basic principles of the development of the information society in Ukraine for 2007-2015”. *Vidomosti Verkhovnoi Rady Ukrainy*, N 12, P.102.
4. The doctrine of information security of Ukraine, approved by Decree of the President of Ukraine 25.02.2017 № 47/2017, available at: <http://president.gov.ua> (Accessed 4 February 2020).
5. On the decision of the National Security and Defense Council of Ukraine dated January 27, 2016 "On the Cybersecurity Strategy of Ukraine": Decree of the President of Ukraine dated March 15, 2016. № 96/2016, available at: <https://zakon.rada.gov.ua/laws/show/96/2016#n11> (Accessed 4 February 2020).

6. Apetik A. (2019) "The information security", available at: [https://webcache.googleusercontent.com/search?q=cache:nY\\_Tl2\\_Dяn-8J:https://www.prostir.ua/%3Flibrary%3Dinformatsijna-bezpeka-now-yakyh-elementiv-ne-vystachaje+&cd=3&hl=ru&ct=clnk&gl=ua](https://webcache.googleusercontent.com/search?q=cache:nY_Tl2_Dяn-8J:https://www.prostir.ua/%3Flibrary%3Dinformatsijna-bezpeka-now-yakyh-elementiv-ne-vystachaje+&cd=3&hl=ru&ct=clnk&gl=ua), (Accessed 5 February 2020).
7. Bogush V.M., Yudin O.K. (2005), "The information security of the state", Kyiv, Ukraine.
8. Zaharenko K. (2017), "The main subjects and institutions of information security", *Naukovyj visnyk*, vol. 48, pp. 212–219.
9. Ilnicka U. (2016) "The information security of Ukraine: current challenges, threats and mechanism of countering negative information and psychological impacts", *Politychni nauky*, Vol. 2, no. 1, 2016, pp. 27–32.
10. Lipkan V.A., Maksimenko Yu.Ye., Zhelihovskij V.M. (2006), "The information security of Ukraine in the context of european integration: textbook", Kyiv, Ukraine.
11. Malik Ya.J., Bereza O.I. (2012), "Ensuring information security of Ukraine in the context of world experience", *Efektivnist' derzhavnoho upravlinnia*, vol. 32, pp. 20–27.
12. Olijnik O.V. (2012), "Administrative legal basis of information security". *Yevropejs'ki perspektyvy*, no. 4(1), pp. 65–68.
13. Panchenko O.A. Banchuk N.V. (2011), "Personal information security: monograph", Kyiv, Ukraine.
14. Prisyazhnyuk M., Byeloshevich Ya. (2013), "Information security of Ukraine in modern conditions", *Visnyk Kyivs'koho natsional'noho universytetu im. T. Shevchenka*, vol. 30, pp. 29–33.
15. Foros G.V., Zhogov V.S. (2019), "Features of the interpretation of the concept of "cybersecurity" in modern legal science", *Pravova derzhava*, no. 33, pp. 128–134.

Стаття надійшла до редакції 20.11.2019 р.