

15. Цивільний процесуальний кодекс України від 15 грудня 2017 р. // Відомості Верховної Ради України. – 2004. – № 40–42. – Ст. 492.

16. Кодекс України про адміністративні правопорушення від 18 грудня 2017 р. № 8073 // Відомості Верховної Ради Української РСР. – 1984. – Додаток до № 51. – Ст. 1122.

17. Про колективні договори і угоди : Закон України від 1 липня 1993 р. № 3356-XII // Відомості Верховної Ради України. – 1993. – № 36. – Ст. 361.

18. Про порядок вирішення колективних трудових спорів (конфліктів) : Закон України від 3 березня 1998 р. № 137/98-ВР // Відомості Верховної Ради України. – 1998. – № 34. – Ст. 227.

19. Про організації роботодавців, їх об'єднання, права і гарантії їх діяльності : Закон України від 22 червня 2012 р. № 5026-VI // Відомості Верховної Ради України. – 2013. – № 22. – Ст. 216.

Дашутін І. В. Сутність правового забезпечення реалізації законності у трудових відносинах

У статті визначено поняття реалізації законності у трудових правовідносинах. Охарактеризовано сутність правового забезпечення реалізації законності у трудових відносинах.

Ключові слова: правове забезпечення, законність, трудові відносини, праця, працівник.

Dashutin I. The essence of the legal framework for the implementation of legality in labor relations

In the article defined the concept of realization of legality in labor legal relations. The essence of legal support for the implementation of legality in labor relations is characterized.

It is substantiated that the realization of legality in labor relations is a mechanism and a process that functions within the framework of ensuring legality and consists in the introduction of the rules aimed at establishing a regime in which the violation of the provisions of labor legislation is minimized, as well as the application of the relevant rights and responsibilities in this area.

Control bodies as entities of law enforcement perform their functions by conducting labor law compliance inspections. According to their results, appropriate sanctions are applied to business entities and violations of labor legislation are required from employers-offenders. As of today, such supervisory bodies are the State Service for Labor and the State Fiscal Service. The relevant authorities have the widest range of powers to impose sanctions for breach of labor legislation.

Not less important subjects of the lawfulness are courts of general jurisdiction. The latter consider individual disputes of the parties to labor relations and in the event of a violation of labor rights and, accordingly, labor laws, take decisions that protect and restore the violated right. In addition, the guilty party shall reimburse the costs incurred by the other party and compensate for the material and non-pecuniary damage suffered by the injured party. Therefore, the court is one of the most important elements as a mechanism for the implementation of legality in labor relations, and the corresponding wider mechanism of ensuring legality.

The peculiarities of the legal provision of the implementation of legality in labor relations are as follows: 1) is realized both by state authorities and by actors – participants in labor relations; 2) the most interested subject in the implementation of legality is a hired employee; 3) hired workers can realize the legality of labor relations both independently and through trade union organizations, which among the subjects of labor relations have the largest set of instruments-powers; 4) the legal framework for the implementation of legality is regulated both in the Labor Code (in the future TK) and in other legislative acts of labor legislation, as well as other legislative acts; 5) the legal framework for the implementation of legality in labor relations can be characterized as due.

It is concluded that the realization of legality is an important theoretical and practical category, which reveals the essence and content of the corresponding legal regulation of labor legal relations. The latter discloses the means available to the subjects of labor relations and state authorities regarding the requirement and actual implementation of legally significant actions aimed at bringing the public relations into conformity with the formally established actions.

Key words: legal support, legality, labor relations, labor, employee.

УДК 342.5

*Пилип Станіславович Демченко,
аспірант відділу конституційного права
та місцевого самоврядування
Інституту держави і права
ім. В. М. Корецького НАН України*

**КІБЕРНЕТИЧНА БЕЗПЕКА ЯК ВАЖЛИВА СКЛАДОВА ЗАБЕЗПЕЧЕННЯ
ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ УКРАЇНИ**

Постановка проблеми. На тлі зростання загроз і нестабільності у світі постають нові виклики національній безпеці України, зокрема і в інформаційній сфері. У частині 1 ст. 17 Конституції України чітко закріплено, що захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою

всього Українського народу. Свідченням цієї концепції є поява загроз та викликів у сфері кібернетичної безпеки. Таким чином, необхідність забезпечення правового регулювання забезпечення кібернетичної безпеки відіграє суттєву роль для України на геополітичній арені, оскільки маючи приклади втручання у державне життя через критичну кібернетичну та інформаційну інфраструктуру вже не раз показало можливості певних держав вплинути на діяльність інститутів держави в західних країнах, використання у військово-підривних цілях та як розвідно-диверсійного засобу. На підставі того, що основні засади кібернетичної безпеки представлені у нормах Конституції України, ми можемо стверджувати про важливість конституційно-правового регулювання цього питання, оскільки кібернетична безпека є новітньою складовою у системі національної безпеки.

Аналіз останніх досліджень та публікацій. У статті використано напрацювання провідних вітчизняних учених-правників у сфері національної безпеки, інформаційної та кібернетичної безпеки, а саме: В. Антонова, О. Баранова, В. Бутузова, М. Дмитренко, Є. Макарчука, В. Фурмашева.

Мета статті. Основним завданням статті є визначення правової категорії «кібернетична безпека» як сучасної складової національної безпеки, зазначення її конституційних і законодавчих засад, визначення основних завдань та функцій у забезпеченні підтримання сталого стану системи національної безпеки. Крім того, метою статті є дослідження зарубіжного досвіду регулювання кібернетичної безпеки як складової національної безпеки на прикладі Федеративної Республіки Німеччина (далі – ФРН).

Основні результати дослідження. Стрімкий розвиток інформаційних та електронно-обчислювальних технологій, міжнародного інформаційного обміну комп'ютерних мереж, а також інформаційне домінування окремих держав світу характеризується значним зростанням світового кібернетичного протистояння. Основними об'єктами інформаційного впливу можуть бути суспільство загалом, його політичні, соціальні та економічні інституції, органи управління всіх рівнів та інформаційні системи. Необхідно погодитися з думкою М. Дмитренка у тому, що впровадження високих наукомісних технологій, нанотехнологій у всі сфери суспільного життя, де провідна роль належить мікроелектроніці, оптоелектроніці, інформаційним технологіям, новим технологіям виробництва високоякісних матеріалів, активно використовуються для розробки нових зразків високоточної та «високоінтелектуальної» зброї [1, с. 4].

На думку Є. Марчука, людська цивілізація нині живе в епоху, коли основою функціонування суспільства є знання, або так звана Четверта технологічна епоха – значною мірою загадкова і досі до кінця не пізнана, символами якої вже стали комп'ютер та супутник зв'язку. Безперечним є те, що у Четверту технологічну хвилю людський інтелект стає безпосередньою виробничою силою, інформація – найціннішим продуктом, а швидкість і якість зв'язку – визначальними чинниками конкурентоспроможності [2, с. 12].

У цьому і полягає проблематика вироблення відповідної сучасної доктрини національної безпеки та її ефективного правового регулювання, система якої буде охоплювати всі основні життєво важливі напрями діяльності суспільства та держави. На думку В. Антонова, національна безпека виражає стан захищеності життєво важливих інтересів особи, суспільства і держави від внутрішніх та зовнішніх загроз. Відповідну позицію можна простежити через наявні компоненти, які становлять єдину структуру національної безпеки кожної конкретної держави: політична, військова, економічна, інформаційна, ідеологічна та ін. [3, с. 140].

Досліджуючи питання правового регулювання поняття кібернетичної безпеки як сучасного структурного компоненту національної безпеки, необхідно вказати на конституційно-правові основи необхідності її забезпечення. Відповідно до ст. 17 Конституції України захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу [4]. Фактично ця конституційна норма окреслює фундаментальні напрями забезпечення усієї системи національної безпеки України. Оскільки з моменту прийняття Основного Закону минуло 22 роки, перед однією з найважливіших функцій держави постало питання розширення напрямів забезпечення національної безпеки та інтересів. Саме з такого розуміння можна встановити, що будучи складовою інформаційної безпеки, кібернетична безпека є новітнім елементом національної безпеки Української держави на сучасному етапі його розвитку і саме з цього приводу положення ст. 17

Конституції України визначають конституційно-правові основи врегулювання кібернетичної безпеки України.

Водночас необхідно зазначити, що ані в вітчизняному, ані в зарубіжному науковому правничому середовищі немає чіткого визначення тому, чим саме є кібернетична безпека. На думку Д. Франсело, активне використання самої термінології «кібернетична безпека» та «кібербезпека» у наш час призводить до виникнення певних конфузів у керівників структурних департаментів служб безпеки різних держав світу та просто експертів з національної та інформаційної безпеки щодо питання особливості формулювання та порядку застосування цього терміна [5].

Якщо ми розглянемо поняття «кібернетична безпека» з філологічного погляду його складових за допомогою Великого тлумачного словника сучасної української мови, ми можемо знайти таке: «кібернетичний – той що стосується кібернетики; який створено, працює на основі принципів, методів кібернетики», а «безпека – стан, коли кому-, чому-небудь ніщо не загрожує» [6, с. 106, 308].

Сам термін «кібернетична безпека» уперше згадується у нормативно-правових актах уряду США, коли у середині 1990-х років розпочалося широкомасштабне дослідження цієї проблематики. Відтоді у світі було проведено велику кількість міжнародних і різноманітних національних заходів та було закладено початок розробці провідними технологічними державами світу власних стратегій кібернетичної безпеки [7].

У сучасному вітчизняному науковому середовищі існує декілька підходів до визначення поняття «кібернетична безпека». На думку В. Фурашева, кібернетична безпека є станом здібності людини, суспільства і держави щодо запобігання та уникнення спрямованого, передусім – несвідомого, негативного впливу (управління) інформації [8, с. 166]. Як вважає В. Бутузов, під поняттям «кібернетична безпека» необхідно розуміти стан захищеності життєво важливих прав та інтересів людини, суспільства, держави у кібернетичному просторі від внутрішніх і зовнішніх протиправних посягань та загроз таких посягань [9, с. 238]. Варто погодитися з визначенням кібернетичної безпеки відповідно до твердження О. Баранова, який вважає, що це такий стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації [7].

Потрібно зазначити, що, окрім положень Конституції України, на забезпечення кібернетичної безпеки України існує низка нормативно-правових актів, які закріплюють та регулюють систему кібернетичної безпеки в Україні. До таких слід віднести: закони України «Про основи національної безпеки»; «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», Указ Президента України від 26 травня 2015 р. № 287/2015 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року “Про Стратегію національної безпеки України”», Указ Президента України від 24 вересня 2015 р. № 555/2015 «Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року “Про нову редакцію Воєнної доктрини”», Указ Президента України від 15 березня 2016 р. № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію кібербезпеки України”», Закон України від 5 жовтня 2017 р. «Про основні засади забезпечення кібербезпеки України».

Із законодавчого масиву нормативно-правових актів у сфері регулювання кібернетичної безпеки необхідно виокремити Закон України від 19 червня 2003 р. «Про основи національної безпеки України». У ньому комп'ютерна злочинність та комп'ютерний тероризм визначаються одними з основних загроз національної безпеки України (ст. 7). Крім того, забезпечення інформаційного суверенітету України, а також затвердження низки гарантій прав і свобод, пріоритетів у розвитку інформаційної сфери визначаються основними напрямками державної політики в питанні національної безпеки (ст. 8) [11].

Фактично першим нормативно-правовим актом у сфері регулювання кібернетичної безпеки стало рішення Ради національної безпеки і оборони України від 27 січня 2016 р. «Про стратегію кібернетичної безпеки», введеної в дію Указом Президента України від 15 березня 2016 р. Ме-

тою цієї стратегії є створення умов для безпечного використання кібернетичного простору, його використання в інтересах особи, суспільства та держави. У межах п. 4 «Пріоритети та напрями забезпечення кібербезпеки України» Стратегії кібернетичної безпеки були визначені основні пріоритетні напрями її розвитку, яка закріплює необхідність вдосконалення існуючої та створення нових електронних інфраструктур, забезпечення підготовки кадрів та міжнародного співробітництва в галузі кібернетичної безпеки (передусім ЄС та НАТО).

Один із нещодавно прийнятих нормативних актів щодо забезпечення кібернетичної безпеки в Україні є Закон України від 5 жовтня 2017 р. «Про основні засади забезпечення кібербезпеки України». У ньому представлений чіткий категоріальний апарат щодо визначення суттєвих понять, які пов'язані з забезпеченням безпеки при використанні електронних пристроїв та електронно-цифрових систем [11]. Важливим є також те, що вперше на законодавчому рівні у п. 5 ч. 1 ст. 1 було закріплено термін «кібербезпека» – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечується сталий розвиток інформаційного суспільства та цифрового комунікаційного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національної безпеки України у кіберпросторі [12].

Важливо також зазначити, що окрім функції та завдань кібернетичної безпеки, законодавством встановлюється національна система кібернетичної безпеки України, яка складається із таких органів: Міністерство оборони України, Генеральний штаб Збройних сил України, Служба безпеки України, Державна служба спеціального зв'язку та захисту, Національна поліція та Національний банк України.

Окремо в системі державних органів щодо забезпечення кібернетичної безпеки в Україні потрібно віднести утворений у рамках робочого органу Ради національної безпеки та оборони Національний координаційний центр кібернетичної безпеки. Його діяльність регулюється Положенням «Про Національний координаційний центр кібербезпеки» затвердженим Указом Президента України від 7 червня 2016 р. № 242/2016.

Основними завданнями Національного координаційного центру кібернетичної безпеки (далі – Центр) є: аналіз стану кібербезпеки; результатів проведення огляду національної системи кібербезпеки; стану готовності суб'єктів забезпечення кібербезпеки до виконання завдань з питань протидії кіберзагрозам; стану виконання вимог законодавства щодо кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також критичної інформаційної інфраструктури; даних про кіберінциденти стосовно державних інформаційних ресурсів в інформаційно-телекомунікаційних системах тощо (пп. 1 п. 3 Положення) [13].

До складу Центру входять керівник, секретар та інші члени Центру. Керівник Центру за посадою є Секретарем Ради національної безпеки і оборони України. Секретар Центру за посадою є керівник структурного підрозділу Апарату Ради національної безпеки і оборони України, до відання якого віднесені питання кібербезпеки. Членами Центру також є: перший заступник або заступник Міністра оборони України, начальника Генерального штабу Збройних Сил України, Голови Служби безпеки України, Голови Служби зовнішньої розвідки України, Голови Національної поліції України, Голови Національного банку України (за згодою), до відання яких належать питання кібербезпеки, а також начальник Головного управління розвідки Міністерства оборони України, начальник Управління розвідки Адміністрації Державної прикордонної служби України, Голова Державної служби спеціального зв'язку та захисту інформації України (п. 5 Положення) [13].

Надаючи загальну характеристику теоретико-правового розуміння національної безпеки у ФРН потрібно зазначити, що вона формувалася у два етапи: перший (у період з 1949 р. по 1990 р.), коли з утворенням Федеративної Республіки Німеччина (або Західна Німеччина) поступово відроджувалася концепція оборонного характеру задля забезпечення безпеки держави та Західної Європи від радянського впливу та військового вторгнення, та другий (після возз'єднання ФРН та НДР у 1990 р.): визначення новітніх напрямів забезпечення національної та загальноєвропейської політики безпеки та оборони в умовах закінчення Холодної війни.

Особливістю доктрини національної безпеки ФРН є те, що у цій державі відсутній єдиний федеральний нормативно-правовий акт, котрий визначав би всі аспекти національної безпеки та

оборони. Водночас Федеральне міністерство оборони ФРН у 1994 р. видало так звану «Білу книгу», в котрій розкриваються основні концепції національної безпеки сучасної Німеччини. Потрібно зазначити, що цей документ (останнє видання 2016 р.) визначає можливості захищати власні інтереси німецької держави у рамках захисту та оборони на всьому земному шарі з використанням, у разі потреби всіх доступних сил (від політичних заходів до прямого військового врегулювання) [14]. Також важливі положення щодо загального забезпечення національної безпеки містяться у Північноатлантичному договорі від 4 квітня 1949 р. (ФРН є членом військово-політичного блоку 9 травня 1955 р.) та похідних домовленостях держав – членів НАТО.

Розкриваючи сутність правового регулювання кібернетичної безпеки у сучасній ФРН, необхідно першочергово зробити акцент на тому, що нормативно-правова база цієї сфери національної безпеки ФРН активно розвивалася протягом останніх 40 років. Із 70-х років ХХ ст. були розроблені такі визначні законодавчі акти федерального рівня: «Про захист персональних даних» у 1977 р. (нова редакція з 1990 р.); «Про основи надання інформаційних та комунікативних комунікаційних послуг» у 1997 р.; «Про посилення безпеки інформаційних систем» у 2009 році (у цьому нормативно-правовому акті зазначено поняття «критична інфраструктура») [15–17].

Основоположним нормативно-правовим актом, який визначає напрями забезпечення кібернетичної безпеки у ФРН, є «Стратегія забезпечення кібернетичної безпеки ФРН», яка була розроблена Федеральним відомством інформаційних систем та затверджена Федеральним Урядом ФРН у 2011 р. Ця Стратегія визначає категоріальний апарат у сфері кібербезпеки, основні загрози, а також засади протидії втручання у кібернетичний простір німецької держави. Важливою рисою Стратегії є визначення основних її напрямків у вигляді забезпечення військової складової (здійснення розвідувальних та оборонних операцій); захист критичної інфраструктури та забезпечення правоохоронної функції. Вона вказує на системний підхід закріплення кібернетичної безпеки як важливої складової національної безпеки ФРН [18].

До основних органів, які координують забезпечення кібернетичної безпеки у ФРН, потрібно віднести Національний центр кіберзахисту, який підпорядкований Державному секретарю Міністерства внутрішніх справ. Фактично він забезпечує політику реалізації кібернетичної безпеки критичної інфраструктури в державі. Крім того, Стратегія кібернетичної безпеки ФРН передбачає функціонування національної ради кібербезпеки, головним завданням якої є вироблення стратегії державної політики та контроль виконання рішень керівництва держави у сфері протидії кіберзагрозам.

Висновки. Таким чином, дослідивши поняття та сутність кібернетичної безпеки як сучасної складової національної безпеки сучасної держави, можна стверджувати про таке. Реалізація захисту кібернетичної безпеки має велику роль та проблематику у сучасному світі для будь-якої держави. Задля оптимального реагування на всі виклики та загрози, чіткого окреслення питань забезпечення кібернетичної безпеки необхідне розроблення та прийняття чіткої стратегії, у якій вказані основні напрями та мета її реалізації. Досвід ФРН у питанні забезпечення кібербезпеки вказує на складний інституційний характер її забезпечення, утім, є позитивним для України, оскільки на прикладі Стратегії кібернетичної безпеки ФРН мається чітко визначений категоріальний апарат у сфері кібернетичної безпеки, основні виклики та загрози в сфері кібернетичної безпеки та окреслення порядку діяльності системи державних органів, на які покладений обов'язок забезпечення кібернетичної безпеки у ФРН.

Використані джерела

1. Дмитренко М. А. Політична система України: розвиток в умовах глобалізації та інформаційної революції / М. А. Дмитренко ; Нац. пед. ун-т ім. М. П. Драгоманова, Ін-т Оперативної діяльності та держ. безпеки. – К. : Знання України, 2008. – 544 с.
2. Макаруч. Є. К. Україна: нова парадигма поступу: Аналітичне дослідження / Є. К. Макаруч. – К. : Аваллон, 2001. – 216 с.
3. Антонов В. О. Поняття та зміст системи національної безпеки / В. О. Антонов // Держава і право. – 2010. – Вип. 48. – С. 137–144.
4. Конституція України від 28 червня 1996 р. № 294к/ВР-96 [Електронний ресурс]. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80>.

5. *Franscella J.* Cybersecurity vs Cyber Security: When, Why and How to Use the Term / J. Franscella [Електронний ресурс]. – Режим доступу : <http://www.infosecisland.com/blogview/23287-Cybersecurity-vs-Cyber-Security-When-Why-and-How-to-Use-the-Term.html>.
6. Великий тлумачний словник сучасної української мови / укл. О. О. Єрошенко. – Донецьк : Глорія Трейд, 2012. – 864с.
7. *Баранов О. А.* Про тлумачення та визначення поняття «кібербезпека» / О. А. Баранов [Електронний ресурс]. – Режим доступу : <http://www.ippi.org.ua>.
8. *Фурашев В. М.* Кібернетичний та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності / В. М. Фурашев // Інформація і право. – 2012. – №2. – С. 162–169.
9. *Бутузов В. М.* Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : моногр. / В. М. Бутузов. – К. : КИТ, 2010. – 408 с.
10. Про основи національної безпеки України : Закон України від 19 червня 2003 р. № 964-IV [Електронний ресурс]. – Режим доступу : <http://zakon5.rada.gov.ua/laws/show/964-15>.
11. Про рішення РНБО України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15 березня 2016 р. № 96/2016 [Електронний ресурс]. – Режим доступу : <http://zakon3.rada.gov.ua/laws/show/96/2016>.
12. Про основні засади забезпечення кібербезпеки України : проект Закону України від 5 жовтня 2017 р. 2163-VIII [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657.
13. Про затвердження Положення «Про Національний координаційний центр кібербезпеки» : Указ Президента України від 7 червня 2016 р. № 242/2016 [Електронний ресурс]. – Режим доступу : <http://zakon5.rada.gov.ua/laws/show/242/2016>.
14. Weißbuch der die Grundlage für die deutsche Sicherheitspolitik 2016 [Електронний ресурс]. – Режим доступу : <https://www.bmvg.de/de/themen/weissbuch>.
15. Bundesdatenschutzgesetz (BDSG) vom 20.12.1990 [Електронний ресурс]. – Режим доступу : <http://www.gesetze-iminternet.de>.
16. Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (IuKDG) vom 20.12.1990 [Електронний ресурс]. – Режим доступу : <http://www.gesetze-iminternet.de>.
17. Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes vom 14.08.2009 [Електронний ресурс]. – Режим доступу : <https://www.bsi.bund.de>.
18. Cyber-Sicherheitsstrategie für Deutschland vom 23.02.2011 [Електронний ресурс]. – Режим доступу : <https://www.bsi.bund.de>.

Демченко П. С. Кібернетична безпека як важлива складова забезпечення інформаційного суверенітету України

У статті розкривається поняття та сутність кібернетичної безпеки як новітньої складової національної безпеки. Окреслюються основні причини необхідності її забезпечення в Україні відповідно до наявних загроз, які на сьогодні мають місце в світі. Проаналізовано низку вітчизняних нормативно-правових актів, які є законодавчою базою забезпечення кібернетичної безпеки України. Для порівняльної характеристики представлений короткий правовий аналіз реалізації забезпечення кібернетичної безпеки у ФРН. Враховуючи відповідні результати правового аналізу та порівняльно-правової характеристики України та ФРН, необхідно стверджувати про необхідність подальшого вдосконалення правового регулювання кібернетичної безпеки як новітньої складової національної безпеки, що забезпечує інформаційний суверенітет України в кібернетичному просторі.

Ключові слова: кібернетична безпека, національна безпека, критична інфраструктура, виклики і загрози стратегії кібернетичної безпеки України.

Demchenko P. Cybernetic safety as a constituent of providing of informative sovereignty of Ukraine is important

The article reveals the concept and essence of cybernetic security as the newest component of national security. The main reasons for the need to provide it in Ukraine are outlined in accordance with the existing threats that are taking place in the world at the moment, among which are aggression of Russian Federation on Ukraine, rising of cyberterrorism and using of cyberspace as new battlefield in XXI century. All this underlines the importance of the need for legal research on this topic. A number of ukrainian normative legal acts, which are the legislative basis for ensuring cybernetic security of Ukraine, are analyzed. For comparative characteristics, a legal analysis of the implementation of the provision of cybernetic security in the Federal Republic of Germany is presented. Based on the results of the legal analysis of Ukrainian legislation and comparative legal characteristics of Ukraine and the Federal Republic of Germany can be argued about the need for further improvement of legal regulation of cyber security as the newest of the national security Institute in Ukraine, which is aimed at providing information sovereignty of Ukraine in cyberspace. It must specify that the challenges and threats that arise with the development of modern technology requires from the legislator for the development of flexible strategies and legislation that could timely immediately stop any negative impact on critical cyberinfrastructure of Ukraine, which in turn will provide stability in the functioning of the Ukrainian state. In this aspect explains the necessity of further study of cyber security as a promising direction in the technical field, but also from the point of view of juridical Sciences.

Key words: cybersecurity, national security, critical infrastructure, challenges and threats for the strategy of cybersecurity of Ukraine.

ТЕОРЕТИЧНА ХАРАКТЕРИСТИКА ДЕРЖАВИ ЯК СУБ'ЄКТА ПРАВА СОЦІАЛЬНОГО ЗАБЕЗПЕЧЕННЯ

Постановка проблеми. На сьогодні в нашій державі відбуваються радикальні зміни у відносинах держави і суспільства. Розвиток України як соціальної правової держави спонукає до налагодження відносин партнерства та співробітництва між державою й кожною окремою особистістю. Водночас існують сфери, у яких особа є повністю залежною від держави та її політики. Однією з таких є соціальне забезпечення, у якому держава є суб'єктом, що надає допомогу, а особа – суб'єктом, який її отримує. Держава, захищаючи права громадян, використовує цей інститут для взаємодії з ними та забезпечення власних інтересів. Проте більш очевидним є значення того захисту від соціальних ризиків, який надається особам, що потребують підтримки і допомоги з боку суспільства та держави.

Державна система соціального забезпечення поступово стає механізмом, у якому основними суб'єктами є держава, фізичні особи та роботодавці. Якщо сутність двох останніх категорій у праві соціального забезпечення постійно досліджується на науковому рівні, то держава залишається суб'єктом, поняття, сутність та ознаки якої як суб'єкта права соціального забезпечення є невстановленими та загалом характеризуються низьким рівнем доктринальної уваги. Все зазначене свідчить про необхідність заповнення цієї теоретичної прогалини, а також про актуальність дослідження питань, пов'язаних із правом соціального забезпечення у сучасних умовах.

Специфічний характер держави як суб'єкта права соціального забезпечення проявляється у тому, що реалізацію її функцій здійснюють спеціально створені для цього органи. Масштабність права соціального забезпечення спричинила впровадження широкого кола суб'єктів, які здійснюють відповідні функції. У зв'язку з цим постає потреба наукового дослідження поняття, сутності та ознак держави як суб'єкта права соціального забезпечення, оскільки питання, пов'язані з характеристикою статусу навіть окремих суб'єктів права соціального забезпечення, є малодослідженими. На сьогодні невстановлена навіть сутність відмінностей між окремими суб'єктами, а переважна більшість досліджень у цій сфері ґрунтується на цивілістичному баченні суб'єктів правових відносин. Саме тому поняття, сутність та ознаки держави як суб'єкта права соціального забезпечення потребують встановлення, а вже розроблені у правовій доктрині елементи – теоретичного переосмислення.

Аналіз останніх досліджень та публікацій. Загалом це питання є новим для вітчизняної науки і досліджувалося лише як елемент більш загальних наукових інститутів. Серед дослідників, які зверталися до його аналізу, варто назвати таких: Н. Болотіна, В. Буряк, С. Жадан, М. Іншин, В. Костюк, О. Кульчицька, П. Пилипенко, С. Прилипко, С. Синчук, І. Сирота, Б. Сташків, О. Тищенко, І. Ярошенко, О. Ярошенко та багато інших. Водночас у вітчизняній науковій літературі ця проблема переважно розглядається у контексті місця держави серед інших суб'єктів права соціального забезпечення, тоді як її поняття та сутність залишаються невизначеними, що й актуалізує необхідність дослідження цієї теми.

Метою статті є розкриття сутності держави як суб'єкта права соціального забезпечення і надання науковій інтерпретації цьому питанню.

Основні результати дослідження. Суб'єктом права соціального забезпечення є індивідуально визначена особа, соціальна група чи організація, що володіє суб'єктивними юридичними правами та обов'язками у сфері соціального забезпечення та галузевим правовим статусом, здійснює цілеспрямовану діяльність, здатна виробляти, виражати та виконувати волю і наділена можливістю брати участь у правовідносинах соціального забезпечення.

Із цієї дефініції можна зробити висновок, що суб'єктам права соціального забезпечення притаманні такі ознаки: 1) персоніфікація – конкретно визначена особа, соціальна група чи організація;