Vasilenko O. V. Data on the system of electronic payments as a subject of a crime

The article reflects the problematic issues of evaluating data of electronic payment systems as a crime subject. The main features of the subject as the necessary element of the corresponding crime are analyzed. The peculiarities of computer information as a subject of crimes in the field of bank payments are determined. A comprehensive list of data of electronic payment systems that can act as a crime subject to the generic features of each specific category of crime, where such data may be involved, is provided. Specific features of such objects as «electronic money» and «money surrogates» as the subject of a crime are determined. At the same time a number of problematic features of the current Ukrainian legislation are identified, which are a medium for the development of criminal activities with information from electronic payment systems. A number of conclusions and recommendations have been prepared to improve the current legislation of Ukraine to prevent this category of crimes.

It has been determined that the data of electronic payment systems is a multi-component and diverse subject of crimes, which is conditioned by the different direction of criminal encroachment on purpose, and the heterogeneity of these electronic payment systems by themselves. When describing these electronic payment systems as criminal offenses, the relevant category should not be narrowed down to a particular type or category of criminal offenses, since with the development of technical progress and the evolution of social relations, various electronic computing systems are closely integrated into the everyday life of a person, thus, appeared quite a large number of syllables of criminal offenses, which in one way or another affect the data of electronic computing systems as a subject of a criminal offense. The legislative framework for the regulation of electronic payment systems in Ukraine has some inaccuracies and gaps, in particular, there is no general legal definition of the concept of an electronic payment system, and, to the end, the legal status of such data is not regulated as a cryptographic currency. In order to improve the methods of investigating economic, economic, property crimes and crimes in the field of cybernetic security, further theoretical development and elaboration of issues related to the consideration of innovative technological progress in public life, in particular regarding the legal status of various types of data in electronic computing systems, should be continued.

Key words: data, information, electronic payment systems, operating systems, cyber security, crime, criminal offense, crime subject, crypto currency, money surrogate.

DOI: 10.33.66.3/2524-017X-2019-10-292-298

УДК 342.5

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

ПРАВОВИЙ МОНІТОРИНГ ВІТЧИЗНЯНОГО ЗАКОНОДАВСТВА В СФЕРІ РЕАЛІЗАЦІЇ СТРАТЕГІЇ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ УКРАЇНИ

Постановка проблеми. Питання забезпечення кібернетичної безпеки України обумовлено двома об'єктивними факторами. Впровадження сучасних технологічних досягнень науково-технічного прогресу в діяльності органів державної влади призвело до необхідності забезпечення захисту їх критичної інфраструктури, яке полягає у вироблені технічних, та що не менш важливо, юридичних напрямках. Другий фактор. Відповідно наша держава потребує вироблення сталої Стратегії та законодавчої основи кібербезпеки з окресленням найважливіших питань її забезпечення. Втім, враховуючи складність технічної термінології та стрімкого розвитку правовідносин в інформаційній сфері, об'єктивним є завдання необхідності проведення правової оцінки відповідного законодавства.

Аналіз останніх досліджень та публікацій. Питання правового моніторингу вітчизняного законодавства неодноразово підіймалося в рамках дослідження юридичної сутності поняття «кібернетична безпека» та захисту інформації у працях вітчизняних спеціалістів з зазначеної проблематики: О. А. Баранов, І. В. Діордіца, Л. В. Єрьоміна, Т. А. Костецька, В. А. Ліпкан, В. П. Шеломенцев,

В. М. Фурашев та інші.

Мета статті. Визначити значення правового моніторингу як юридичного засобу вдосконалення вітчизняного законодавства щодо правового регулювання в сфері інформаційних відносин та кіберпростору.

Основні результати дослідження. Перш ніж перейти до дослідження сутності правового моніторингу вітчизняного законодавства в сфері кібернетичної безпеки в рамках національної безпеки України, слід надати оцінку поняттю правового моніторингу в юридичній науці, меті та основним способам застосування. Відповідне націлено на окреслення загальних рис явища «правового моніторингу», які за своєю суттю використовуються при дослідженні конкретного питання, на основі котрого виробляються ефективні шляхи його вирішення.

Моніторинг (від англ. monitoring) – система спостережень, оцінки, прогнозу стану та динаміки будь-якого явища, процесу чи об'єкта з метою контролю, управління його станом, охорони, виявлення його відповідності бажаному результату чи первинним стандартам [1, с. 502]. Наведене енциклопедичне визначення поняття «моніторинг» закріплює загальні ознаки даного явища в ракурсі його використання будь-яких видів діяльності. Необхідно зазначити, що на сьогодні у вітчизняній юридичній науці відсутній єдиний підхід до визначення терміна «правовий моніторинг», оскільки зазначена категорія залежить від конкретної сфери правовідносин чи об'єкта стосовно котрого застосовуються заходи правового моніторингу. Але разом з тим, деякими науковцями подається власне бачення загального визначення «правовий моніторинг». На думку І. Д. Шустака, правовий моніторинг – це основна ланка механізму реалізації правотворчої політики, яка використовує такі інструменти забезпечення високої якості нормативно-правових актів, як соціологічні дослідження, обробку та аналіз статистичних даних, прогнозування і моделювання дії майбутніх законів, комплексну оцінку законопроектів [2, с. 50]. Ю. В. Градова вважає, що правовий моніторинг є злагодженим механізмом, що дозволяє встановити стійкий зв'язок між законодавчою діяльністю та її кінцевим результатом, перш за все, з метою удосконалення і розвитку національного законодавства [3, с. 47].

З наведених вище визначень правового моніторингу можна зробити первинні висновки у тому, що засоби та способи реалізації спрямовані на забезпечення аналізу нормативно-правової бази в державі з метою виявлення правових недоліків, які суттєво можуть вплинути на застосування конкретного нормативно-правового акта. У даному разі мету правового моніторингу нормативно-правових актів необхідно розглядати, з одного боку – як засіб підвищення ефективності нормативно-правових актів (тактична складова), а з іншого – підвищення ефективності роботи механізму всього правового регулювання (стратегічна) [4, с. 47]. Забезпечення перевірки нормативно-правового акта, в першу чергу, грає велику роль для можливості його чіткого використання при регулюванні суспільно-правових відносин.

Переходячи до розгляду застосування правового моніторингу загроз кібернетичній інфраструктурі виборчого процесу, першочергово необхідно зазначити чинники, які призвели необхідність утворення комплексного забезпечення кібернетичної безпеки виборчого процесу в Україні, як у технічному, так і нормативно-правовому напрямках. Одним із прикладів використання органами державної влади сучасних інформаційних технологій можна назвати проведення виборчого процесу із застосуванням комп'ютерних пристроїв та електронно-автоматизованих систем, які покликані забезпечити ефективне функціонування баз даних виборчого процесу, передачу даних та підрахунку голосів виборців. Разом з тим світова практика свідчить про необхідність забезпечення якісного нормативно-правового закріплення протистояння сучасним викликам та загрозам у зв'язку з активним використанням електронних технологій задля втручання у виборчий процес.

Одними з таких прикладів можна назвати хакерські атаки типу «відмова в обслуговуванні» в М'янмі напередодні парламентських виборів 2010 року, які призвели до збою у роботі мережі «Інтернет». На даний момент не встановлено звідки виконувався підрив функціонування мережі (деякими західними експертами з питання кібернетичної безпеки наводяться факти, що дана атака носила зовнішній характер в інтересах правлячої з 1988 року військової хунти з використанням сучасних військових потужностей даної держави в кібернетичній сфері. Як результат – більшістю держав світу дані вибори були визнані фіктивними, а сама хакерська атака – однією з найпотужніших за останні 10 років [5].

Також прикладом втручання у виборчий процес можна назвати хакерську атаку на штаб демократичної партії США у липні 2016 року, який протягом місяця зазнав втручання до серверів

від кіберзлочинців, результатом котрого стали три зломи бази даних партії, а також розголошення електронного листування між демократами, даних щодо виборів до Конгресу, а також отримання доступу до програм обробки даних після атаки на сервер Національного комітету демократичної партії [6]. Через місяць подібних атак зазнав штаб республіканської партії, але через захищеність як державними службами, так і приватними компаніями, основної мети дана атака не досягла, хоча певним чином вказується, що основним завданням було створити збій у електронній системі республіканців [7]. Крім того, останніми даними розслідувань, вказується про хакерські атаки на 39 штатів у день голосування. Основною метою даної атаки було зламування програмного забезпечення виборчого процесу, а також отримати доступ до бази даних списків виборців [8]. Дані події вказують на той факт, що в Сполучених Штатах одразу після завершення виборчих перегонів 2016 року почалася розробка нових методів та стратегічних підходів щодо захисту національної кібернетичної безпеки в сфері захисту критичної інфраструктури виборчого процесу. Разом з тим стає очевидним, що можливість впливу на виборчий процес шляхом інформаційних технологій у веденні нового типу кібернетичного протистояння в сучасному світі.

Зазначені приклади свідчать про необхідність розроблення Україною ефективної та гнучкої Стратегії кібернетичної безпеки, яка покликана в першу чергу давати чітку характеристику існуючим та перспективним ризикам, загрозам та викликам її кібернетичної інфраструктури. Реалізація зазначеного забезпечить можливість розробки підвідомчих актів органів, які, засновуючись на нормах положень системи національного законодавства в сфері кібернетичної безпеки, оптимізують використання сучасних комп'ютерних технологій та електронних систем і мереж.

Але разом з тим на сьогодні існує проблематика формулювання термінологічних основ, принципів, окреслення завдань та повноважень суб'єктів забезпечення безпеки України в кібернетичному просторі. Це пов'язано фактичною відсутністю чіткого юридичного визначення, якими апелює кіберпростір.

Наразі в вітчизняній науці існує низка визначень, які ґрунтуються на технічній специфіці та націлені на правове обґрунтування відповідної термінологічної бази. Розглядаючи розуміння самого терміна «кібернетична безпека», досить вдалими можна назвати визначення ряду вітчизняних дослідників. На думку О. А. Баранова, пропонує визначати термін «кібербезпека» як стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних систем [9]. В. М. Фурашев визначає поняття «кібернетична безпека» як стан здібності людини, суспільства і держави щодо запобігання та уникнення спрямованого. В першу чергу – несвідомого, негативного впливу (управління) інформації [10, с.166]. Дані визначення характеризуються зазначенням технічної та соціально-інформаційної складових реалізації інформаційної політики та Стратегії кібербезпеки України. Разом з тим нерідко буває, коли законодавець уникає окреслення відповідних категорій у конкретній правовій нормі, утворюючи таким чином розбіжності з об'єктом правового регулювання.

На сьогодні нормативна база в сфері забезпечення кібернетичної безпеки складається з: Конституції України від 28.06.1996 р., Законів України: «Про національну безпеку України» від 21.06.2018 р; «Про інформацію» від 02.10.1992 р., «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 р., «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р., Указу Президента України «Про рішення РНБО від 06.05.2015 р., «Про стратегію національної безпеки України» від 26.05.2015 р. № 287/2015, Указу Президента України «Про рішення РНБО від 02.09.2015 р., «Про нову редакцію Воєнної доктрини» від 24.09.2015 р. № 555/2015 р., Указу Президента України «Про рішення РНБО від 27 січня 2016 року «Про Стратегію кібербезпеки України» від 15 березня 2016 року № 96/2016 та інших нормативно-правових актів.

Особливу увагу з відповідного нормативно-правового масиву регулювання правовідносин в сфері кіберпростору слід приділити Закону України «Про основи кібернетичної безпеки України» № 2163-VIII від 05.10.2017 року. Особливість цього Закону полягає у закріпленні ст. 1 категоріального апарату в сфері забезпечення кібернетичної безпеки в Україні, а відповідно до п. 5 ч. 1 ст. 1 кібербезпека визначається як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпро-

сторі. Також необхідно вказати, що концепція забезпечення кібернетичної безпеки України в зазначеному Законі полягає у її забезпеченні побудови національної системи кібернетичної безпеки, в основу котрої покладені реалізація управлінських та технологічних підходів щодо її реалізації державою в інформаційному, економічному, політичному, військових напрямках. Важливою рисою Закону України «Про основні засади забезпечення кібернетичної безпеки України» від 05.10.2017 р. є визначення основних засад забезпечення інтересів людини та громадянина, суспільства та держави, закріплення повноважень органів державної влади, підприємств, установ та організації в сфері забезпечення кібернетичного простору України (ст. 5); принципів забезпечення кібернетичної безпеки України (ст. 7); основних об'єктів, які складають критичну інфраструктуру України (ст. 6); закріпляє положення щодо національної системи кібернетичної безпеки України (ст. 8) [11].

Прийняття відповідного Закону є результатом багаторічної праці законодавця, який привів до прийняття фахового нормативно-правового акта щодо основних напрямків забезпечення кібернетичної безпеки України.

Разом з тим на сьогодні існує критика щодо нормативно-правового формулювання деяких положень відповідного Закону. До такого прикладу можна навести закріплення термінів в п. 7 та п. 11 ч. 1 ст. 11 Закону «кіберпростір» та «кіберзагроза» для котрих наразі не існує загального юридичного визначення, що на думку Л. В. Єрьоміної, призводить до відсутності термінологічної єдності [12, с. 70-71]. Як зазначає І. В. Діордіца, недоліки категоріального апарату Закону не дозволяють у практичній діяльності: 1) визначити ознаки та індикатори з метою об'єктивної оцінки існуючих, реальних та потенційних загроз та небезпек у національному сегменті кіберпростору України; 2) унеможливлення визначення структурно-функціональних найбільш ефективних заходів забезпечення кібернетичної безпеки в рамках кібербезпекової політики; 3) чіткого визначення переліку компетенції суб'єктів кібернетичної безпеки [13, с. 295]. На думку В. П. Шеломенцева, нечітке формулювання понятійного апарату у сфері забезпечення кібернетичної безпеки не дозволяють визначити ознаки та об'єктивно оцінити основні загрози у національному сегменті кіберпростору та визначити найбільш ефективні підходи для забезпечення кібернетичної безпеки, що передбачає чітке окреслення завдання та функції суб'єктів кібернетичної безпеки [14, с. 313].

На основі аналізу деяких положень Закону України «Про основи кібербезпеки України» від 07.10.2017 р. необхідно вказати на відсутності чіткого законодавчого формулювання технічної термінології, яка використовується для окреслення явищ та процесів в сфері кіберпростору. На думку Т. А. Костецької, така відсутність узгодженого категоріально-понятійного апарату, неналежна увага цієї проблеми науковців та законодавця до відповідної проблематики є наслідком низької законодавчої техніки, яка веде до нечітко сформульованого законодавства направленого на врегулювання інформаційних правовідносин [15, с. 279].

Зазначивши основні проблематичні риси формулювання нормативно-правових основ щодо регулювання правовідносин в сфері реалізації політики кібернетичної безпеки, необхідно зазначити, що у даному випадку застосування правового моніторингу необхідно розглядати в ракурсі засобу вдосконалення та оцінки вітчизняного законодавства при його розробці чи внесенні поточних змін.

В аспекті розвитку сучасних інформаційних правовідносин та наявності все більш перспективних загроз та ризиків кібернетичної безпеки України, доцільним є застосування наступних підходів перевірки нормативно-правових актів:

забезпечення чіткого формулювання юридичних понять щодо термінології, пов'язаної із забезпечення кібернетичної безпеки на основі впливу сучасних інформаційних технологій.

Проведення характеристики стану розвитку соціально-інформаційних відносин в суспільстві.

Утворення оптимальної системи законодавства, яка окреслює основні напрямки забезпечення реалізації стратегії кібернетичної безпеки України на основі вищезазначених підходів.

Оцінки поточного стану реалізації положень щодо забезпечення кібернетичної безпеки з урахуванням існуючих та перспективних загроз та ризиків.

Висновки. Значення правового моніторингу у дослідженні вітчизняного законодавства в сфері реалізації політики кібернетичної безпеки полягає у прямій перевірці правових положень, завдання котрої націлені на визначення неточностей законодавчої техніки щодо визначення понять, якими апелює сфера кібернетики, окреслення об'єкта кібернетичної безпеки, кола суб'єктів забезпечення кібернетичної безпеки та їх завдань.

Список використаних джерел

1. *Тихомирова Л. В.*, Тихомиров М. Ю. Юридическая энциклопедия. Изд. 5-е, доп. и перераб. / Под ред. М. Ю. Тихомирова. – М., 2007. – 972 с.
2. *Шустак І. Д.* Правовий моніторинг: застосування прогностичного методу// І. Д. Шустак // Філософські та методологічні проблеми права. – 2014. – №2. – С. 47-57.
3. *Градова Ю. В.* Щодо необхідності розробки та прийняття Закону України «Про правовий моніторинг» / Ю. В Градова // Вісник Харківського національного університету імені В. Н. Каразіна. – Серія «Право». Вип 24. – 2017. – С. 46-48.
4. *Арзамазов Ю. Г.*, Наконечный Я. Е. Концепция мониторинга нормативно-правових актов : моногр. / Ю. Г. Арзамасов, Я. Е. Наконечный. – М. : Изд. «Юрлитинформ», 2011. – 208 с.
5. *Кибервойны* XXI века: самые громкие случаи применения кибернетического оружия [Електронний ресурс]. – Режим доступу: https://www.kommersant.ru/doc/2729773
6. *Штаб* Клинтон подтвердил хакерскую атаку на свою сеть [Електронний ресурс]. – Режим доступу : http://eadaily.com:8080/ru/news/2016/07/30/shtab-klinton-podtverdil-hakerskuyu-ataku-na-svoyu-set
7. *Хакеры* взломали компьютерные сети предвыборного штаба Трампа и других республиканцев [Електронний ресурс]. – Режим доступу : http://www.newsru.com/world/19aug2016/hack.html
8. *Атаки* российских хакеров во время выборов в США затронули 39 штатов LB.Ua [Електронний ресурс]. – Режим доступу : https://lb.ua/world/2017/06/13/368948_ataki_rossiyskih_hakerov_vremya.html
9. *Баранов О. А.* Про тлумачення та визначення поняття «кібербезпека»/ О. А. Баранов [Електронний ресурс]. – Режим доступу : ippi.org.ua
10. *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.
11. *«Про* основні засади забезпечення кібербезпеки України» : Закон України від 05.10.2017 року із змінами та доповненнями станом на 08.07.2018 р. [Електронний ресурс]. – Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657
12. *Єрьоміна Л. В.* Напрями удосконалення законодавства України у сфері кібербезпеки:термінологічний аспект / Л. В. Єрьоміна // Інформаційна безпека:виклики і загрози сучасності : зб. матеріалів науково-практ. конф. (5 квіт., 2015 р., м. Київ) Київ : НВЦ НАСБ України, 2013. – 416 с.
13. *Діордіца І. В.* Адміністративно-правове регулювання кібербезпеки України : дис.. … докт. юрид. наук : 12.00.07, Зап. нац. ун-т., 2018 . – 521 с.
14. *Шеломенцев В. П.* Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення / В. П. Шеломенцев// Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2012. – Вип. 1. – С. 312-320.
15. *Костецька Т. А.* Категоріально-понятійні аспекти чинного законодавства України у сфері інформаційних відносин / Т. А. Костецька // Альманах права. – 2011. – Вип. 2. – С. 278-281.

References

1. *Tikhomirova L.V.*, Tikhomirov M.Yu. Yuridicheskaya entsiklopediya. Izdaniye 5-e, dopolnenoye i pererabotanoye / Pod red. M. Yu.Tikhomirova. – M., 2007. – 972 s.
2. *Shustak I. D.* Pravovyi monitorynh: zastosuvannia prohnostychnoho metodu // I. D. Shustak // Filosofski ta metodolohichni problemy prava. – 2014. – №2. – S. 47-57.
3. *Hradova Yu.V.* Shchodo neobkhidnosti rozrobky ta pryiniattia Zakonu Ukrainy «Pro pravovyi monitorynh» / Yu. V. Hradova // Visnyk Kharkivskoho natsionalnoho universytetu imeni V. N. Karazina, Seryia «Pravo». – Vyp. 24. – 2017. – S. 46-48.
4. *Arzamazov Yu. G.* Nakonechnyy Ya. E. Kontseptsiya monitoringa normativno-pravovikh aktov : monogr. / Yu. G. Arzamasov, Ya. E. Nakonechnyy // M., Izd. «Yurlitinform», 2011. – 208 s.
5. *Kibervoyny* XXI veka: samyye gromkiye sluchai primeneniya kiberneticheskogo oruzhiya. Retrievered from: https://www.kommersant.ru/doc/2729773
6. *Shtab* Klinton podtverdil khakerskuyu ataku na svoyu set'. Retrievered from:http://eadaily.com:8080/ru/news/2016/07/30/shtab-klinton-podtverdil-hakerskuyu-ataku-na-svoyu-set
7. *Khakery* vzlomali kompyuternyye seti predvybornogo shtaba Trampa i drugikh respublikantsev. Retrievered from: http://www.newsru.com/world/19aug2016/hack.html
8. *Ataki* rossiyskikh khakerov vo vremya vyborov v SShA zatronuli 39 shtatov. Retrievered from: https://lb.ua/world/2017/06/13/368948_ataki_rossiyskih_hakerov_vremya.html
9. *Baranov O. A.* Pro tlumachennia ta vyznachennia poniattia «kiberbezpeka»/ O. A. Baranov. Retrievered from: https://ippi.org.ua.
10. *Furashev V. M.* Kibernetychnyi ta informatsiinyi prostir, kiberbezpeka ta informatsiina bezpeka: sutnist, vyznachennia, vidminnosti / V. M. Furashev // Informatsiia i pravo. – 2012. – № 2. – S.162-169.

11. *«Pro* osnovni zasady zabezpechennia kiberbezpeky Ukrainy»: Zakon Ukrainy vid 05.10.2017 roku iz zminamy ta dopovnenniamy stanom na 08.07.2018 roku Retrievered from: //http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657.
12. *Yeromina L.V.* Napriamy udoskonalennia zakonodavstva Ukrainy u sferi kiberbezpeky: terminolohichnyi aspect / L. V. Yeromina // Informatsiina bezpeka:vyklyky i zahrozy suchasnosti: zb. materialiv naukovo-prakt. konf. (5 kivt., 2015 r., m. Kyiv) Kyiv : NVT's NASB Ukrainy, 2013. – 416 s.
13. *Diorditsa I. V.* Administratyvno-pravove rehuliuvannia kiberbezpeky Ukrainy / I. V. Diorditsa //dys. … d.iu.n : 12.00.07, Zap. nats. univ., Zaporizhzhia, 2018. – 521 s.
14. *Shelomentsev V. P.* Pravove zabezpechennia systemy kibernetychnoi bezpeky Ukrainy ta osnovni napriamy yii udoskonalennia / V. P. Shelomentsev // Borotba z orhanizovanoiu zlochynnistiu i koruptsiieiu (teoriia i praktyka). – 2012. – Vyp. 1. – S. 312-320.
15. *Kostetska T. A*. Katehorialno-poniatiini aspekty chynnoho zakonodavstva Ukrainy u sferi informatsiinykh vidnosyn / T. A. Kostetska // Almanakh prava. – 2011. – Vyp. 2. – S. 278-281.

Демченко П. С. Правовий моніторинг вітчизняного законодавства в сфері реалізації Стратегії кібернетичної безпеки України

Стаття присвячена дослідженню ролі правового моніторингу як засобу дослідження нормативно-правових актів в сфері кібернетичної безпеки України. Розкрита загальні сутність та ознаки поняття «правовий моніторинг», роль правового моніторингу як методу дослідження та оцінки законодавства України як на стадії розробки, так й при характеристиці вже діючих правових норм. Важливість необхідності використання правового моніторингу як методологічного засобу вдосконалення існуючого законодавства представлена в ракурсі дослідження законодавства в сфері кібернетичної безпеки у зв'язку з всебічним впровадженням застосування сучасних інформаційних технологій в житті особи, суспільства, держави. В рамках дослідження підіймається проблематика наявності деяких законодавчих прогалин в Законі України «Про основні засади кібербезпеки України» від 07.10.2017 року, в основі котрих полягає відсутність єдності юридичної техніки формулювання категоріального апарату, заснованого на технічній термінології, на котрою апелює сфера кібернетики та інформатики. З окресленої проблематики наводяться підходи щодо проведення правового моніторингу, націленого на виявлення та усунення неточностей у системі нормативно-правових актів в сфері забезпечення кібернетичної безпеки в Україні.

Ключові слова: правовий моніторинг, законодавство, кібернетична безпека.

Demchenko P. S. Legal monitoring of domestic legislation in the field of palalization of the strategy of Ukraine's cibernetic security

This article is devoted to the study of the nature and objectives of the legal monitoring of Ukrainian legislation in the implementation of cyber security policy. The relevance of the topic is explained by the unprecedented in the whole history of mankind the increased role of modern achievements of science and technology – modern information technologies (computer equipment, electronic – automated systems, communication networks, etc.), which in general affect the development of the life of an individual, society, state and the whole world.

In this regard, the role of the need to create a legislative framework in the sphere of legal regulation of the use of modern information technologies, one of the components of which is the implementation of the cyber security of Ukraine, is growing. As an example of a significant threat to the critical infrastructure of Ukraine, the current practice of external interference in the electoral process using computer equipment and networks is shown.

But together with this, the practical implementation of ensuring cyber security requires an essential approach to clearly consolidate the terminological base, which is based on concepts inherent in the science of cybernetics and the information sphere, the distribution of powers of public authorities, the definition of functional areas and tasks in implementing cyber security modern information component of the national security of Ukraine.

That is why it is necessary to conduct preliminary legal monitoring of legislation in the sphere of the implementation of the cyber security policy of Ukraine in order to comply with the existing modern legal relations in the information sphere and to use the high-precision achievements of scientific and technological progress.

Today, the problem of the formulation of regulations for ensuring cyber security, which is enshrined in the Law of Ukraine «On the Basics of Cyber Security of Ukraine» dated 10.07.2017, received ambiguous criticism and requires its review and reform. In this case, it will be relevant to use methods of legal monitoring of the evaluation of draft amendments to this regulatory act, in accordance with the proposed levels of evaluation of the preparation of changes.

Thus, the opinion is given that the essence of legal monitoring of legislation in the field of ensuring the cyber security of Ukraine is to ensure the verification of its compliance with a specific area of legal relations, which, due to its specific nature, requires comprehensive preparation and verification of legal norms.

Key words: legal monitoring, legislation, cyber security.

DOI: 10.33.66.3/2524-017X-2019-10-298-303