СЕКЦІЯ 4
АДМІНІСТРАТИВНЕ ПРАВО І ПРОЦЕС; ФІНАНСОВЕ ПРАВО; ІНФОРМАЦІЙНЕ ПРАВО

УДК 351.86:007.659.2/4(477)
DOI 10.32999/ksu2307-8049/2019-2-4

ОСОБЛИВОСТІ ДЕРЖАВНОЇ ПОЛІТИКИ УКРАЇНИ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Веселова Лілія Юріївна,
кандидат юридичних наук,
доцент кафедри адміністративної діяльності поліції
Одеський державний університет внутрішніх справ
cvet-Liliya@ukr.net
orcid.org/0000-0001-6665-0426

Мета. Під час дослідження визначити проблеми та перспективи правового регулювання кібернетичної безпеки в умовах гібридної війни та виробити на цій основі науково обґрунтовані пропозицій до національного безпекового законодавства України.

Методи. Методологічною основою дослідження є система загальнонаукових та спеціальних методів пізнання, а саме формально-логічний метод, логіко-семантичний метод та метод моделювання.

Результати. У статті проаналізовано особливості державної політики України у сфері забезпечення кібернетичної безпеки в умовах гібридної війни. Після вивчення та аналізу наукових досліджень багатьох провідних учених у галузі адміністративного, конституційного та інших суміжних галузей права щодо проблематики кібернетичної безпеки та державної політики констатовано, що державна політика у сфері забезпечення національної безпеки (кібернетичної безпеки) відноситься до вищого інтегрованого елемента внутрішньої та зовнішньої політики України та являє собою систему цілей, а також сукупність принципів, норм, напрямків та форм діяльності органів державної влади у сфері забезпечення національної безпеки (кібернетичної безпеки) та стійкого соціально-економічного розвитку країни. Охарактеризовано Стратегію національної безпеки України, яка має загальнонаціональний характер та визначає загрози національній безпеці (кібернетичної безпеки) держави, першочерговою з яких у теперішніх складних для системи державного управління умовах виступає агресія Російської Федерації на території України.

Висновки. У статті зроблено висновок, що існує необхідність щодо запровадження системи заходів, які включають: подолання декларативного характеру законодавства і скорочення розриву між законодавством і правозастосовною діяльністю в кібернетичній сфері, уточнення загроз кібернетичної безпеки України, а також утворення нових інститутів на кшталт Національного координаційного центру кібернетичної безпеки, які визначають рамки взаємодії і правил поведінки в Інтернет-просторі. У статті доведено, що окремі недоліки та рамковий характер Доктрини інформаційної безпеки України знижують ефективність і обмежують сферу її застосування, визначають хибний напрямок розвитку законодавства в кібернетичної сфері та вносять плутанину в процесі його застосування. У статті робиться висновок, що для належного забезпечення кібернетичної безпеки доцільним буде утворення відповідної системи правових відносин, що, у свою чергу, неможливо без перегляду категоріального апарату, доктринального і концептуального фундаменту законодавства в інформаційній сфері.

Ключові слова: *інформаційна сфера, національна безпека, інформаційне суспільство, кібернетичний простір, кібернетичні загрози.*

PECULIARITIES OF THE STATE POLICY OF UKRAINE IN THE FIELD OF PROVIDING CYBER SECURITY IN CONDITIONS OF HYBRID WAR

Veselova Liliya Yuriivna,
Candidate of Law Sciences,
Associate Professor of the Department of Police Administration
Odessa State University of Internal Affairs
cvet-Liliya@ukr.net
orcid.org/0000-0001-6665-0426

Purpose. During the research to identify problems and prospects of legal regulation of cyber security in the conditions of hybrid war and to make on this basis scientifically substantiated proposals to the national security legislation of Ukraine.

Methods. The methodological basis of the research is the system of general scientific and special methods of cognition, namely, formal-logical method, logical-semantic method and method of modeling.

Results. The article analyzes the peculiarities of the state policy of Ukraine in the sphere of providing cyber security in the conditions of hybrid war. After studying and analyzing the scientific research of many leading scientists in the field of administrative, constitutional and other related branches of law on cyber security issues and public policy, it is ascertained that state policy in the field of national security (cyber security) is a higher integrated element of internal and foreign Ukraine. and is a system of goals, as well as a set of principles, norms, directions and forms of activity of public authorities in the sphere of providing tion of national security (cyber security) and sustainable socio-economic development. The National Security Strategy of Ukraine, which has a national character and identifies threats to the national security (cyber security) of the state, of which the aggression of the Russian Federation on the territory of Ukraine is a priority in the present difficult for the state administration system, is characterized.

Conclusions. There is a need to introduce a system of measures, including: overcoming the declarative nature of legislation and reducing the gap between legislation and law enforcement activities in the cyber sphere, clarification of cyber security threats to Ukraine, as well as the creation of new institutions such as the National Cyber Security Coordination Center, rules of conduct in the Internet space. The article proves that some of the shortcomings and framework nature of the Doctrine of Information Security of Ukraine reduce the effectiveness and limit its scope, determine the wrong direction of the development of legislation in the cybernetic sphere and make confusion in the process of its application. The article concludes that in order to properly ensure cyber security, it would be advisable to create an appropriate system of legal relations, which, in turn, is impossible without reviewing the categorical apparatus, the doctrinal and conceptual foundations of legislation in the information field.

Key words: *informatsiyna sfera, national security, information society, cyber space, cyber threats*

1. Вступ

Інформаційна сфера у якості системоутворюючого фактору розвитку суспільства активно впливає на політичну, економічну, оборонну та інші складові елементи системи національної безпеки України. У той же час національна безпека держави значною мірою залежить від стану забезпечення безпеки інформаційної.

Слід констатувати, що динамічне формування глобального інформаційного простору пов'язано, з одного боку, з наданням суспільству унікальних інформаційних можливостей, а з іншого – з виникненням нових загроз в інформаційній сфері суспільних відносин. Із появою нового феномену кібербезпеки з'явилися сучасні правові категорії «кіберзлочинність», «кібертероризм», «кібервійна», які слугують віддзеркаленням сучасного стану захищеності суспільства.

Поряд із цим із часів проголошення незалежності української держави національна кібернетична безпека розглядалась найвищими посадовими особами органів державної влади в якості недооціненого та, як наслідок, недостатньо розвиненого напрямку забезпечення національної безпеки України. Відповідна тенденція спостерігалась і у правовому полі держави, коли кібернетична безпека фактично не згадувалась у нечисленних законодавчих актах серед основних загроз національній безпеці країни.

Проблематика кібернетичної безпеки та державної політики, спрямованої на її забезпечення, виступала предметом наукових досліджень багатьох провідних учених у галузі адміністративного, конституційного та інших суміжних галузей права, як-от: В.Б. Авер'янова, І.В. Арістової, І.Л. Бачило, І.П. Голосніченка, О.Д. Довганя, Р.О. Додонова, І.М. Дороніна, Л.В. Кузенка, О.Є. Кутафіна, В.Л. Манілова, О.В. Нестеренка, Г.В. Падалка, В.П. Пєткова, С.В. Пєткова, В.Л. Сидоренко, О.Ю. Синявської, С.Г. Стеценка, В. Тертичка, М.М. Тищенка, Ю.П. Тихомірова, О.М. Шевчука, В.К. Шкарупи, та інших. У той же час науковий пошук у вищевказаному напрямку в умовах проведення на території України гібридної війни залишається недостатньо розробленим.

2. Сучасний стан державної політики у сфері забезпечення кібернетичної безпеки України

Кардинальні зрушення в державній політиці щодо вдосконалення кібербезпеки України розпочались у 2014 році, з початком збройної агресії РФ на території України. Зазначені фактори змусили українське суспільство визнати кібербезпеку одним із ключових елементів системи національної безпеки держави. Зазначений факт, зокрема, підтверджується й висновком Р.О. Додонова, який наголошує на входженні України до найскладнішого періоду свого розвитку. Вчений зазначає, що поряд із низкою країн світової спільноти Україна вперше у своїй історії зіткнулась із необхідністю організації оборони в умовах інформаційного суспільства, коли інформаційно-психологічний вплив став головним чинником ведення сучасної війни, яка отримала назву «гібридної» (Гібридна війна: in verbo et in praxi, 2017: 135).

Як наслідок, значення інформаційної складової частини в системі національної безпеки наразі суттєво зростає. Відповідно до частини 4 статті 3 Закону України «Про національну безпеку» кібербезпека України визначається в якості одного з головних об'єктів державної політики у сфері національної безпеки (Про національну безпеку: закон України від 21.06.2018 № 2469-VIII. 2). Особливість інформаційної безпекової сфери полягає в тому, що окремі її складові частини присутні у всіх без виключення напрямках забезпечення національної безпеки. Зокрема, попри те, що відповідно до частини 4 статті 3 Закону України «Про національну безпеку» в напрямку реалізації державної політики кібербезпека виокремлена у самостійний напрямок національної безпеки, її забезпечення є

необхідною умовою під час реалізації воєнного, зовнішньополітичного, державного, економічного, інформаційного та екологічного напрямків національної безпеки. Тобто в даному випадку ми можемо говорити про універсальний характер функції забезпечення кібербезпеки, адже стрімкий розвиток та широке розповсюдження сучасних інформаційних технологій відбувається не тільки у сфері національної безпеки країни, але й у суміжних сферах суспільних відносин, які мають принципове значення для ефективного забезпечення безпеки сучасної держави.

Таким чином, інформаційна складова частина посідає важливе місце серед засобів забезпечення національної безпеки, а її значення й надалі зростатиме в механізмі державного регулювання суспільно-політичних процесів, як мінімум, у середньостроковій перспективі.

За висловленням О.Д. Довганя та І.М. Дороніна, кібербезпека все частіше розглядається як стратегічна проблема державного рівня, зачіпає всі верстви суспільства. На думку авторів, державна політика кібербезпеки повинна служити засобом посилення безпеки та надійності інформаційних систем держави (Довгань, 2017: 9).

Теоретичне розуміння формування державної політики як процесу організації та реалізації публічного управління в різних сферах суспільних відносин доволі докладно з'ясовано вітчизняними та зарубіжними науковцями. Наприклад, В. Тертичка підкреслює надзвичайну важливість державної політики у процесі організації суспільного життя, спрямовану на своєчасне виявлення назрілих проблем розвитку суспільства, їхній аналіз, встановлення причин їхнього виникнення, визначення їхньої складності, суперечливості та винайдення шляхів їх вирішення. Вчений наголошує, що мета державної політики головним чином спрямована на прийняття державно-політичних рішень, призначених вирішувати різноманітні проблемні аспекти суспільно-політичного життя (правові, політичні, соціальні, економічні, екологічні, культурні тощо), та які слугують підставою для вироблення органами державної влади дієвих механізмів їх реалізації (Тертичка, 2002: 5).

О.Є. Кутафін підкреслює яскраво виражені функціональні властивості державної політики, яка, на думку автора, являє собою «визначений органом державної влади напрям діяльності, спрямований на вирішення певної проблеми або їх сукупності» (Кутафин, 2001: 358).

Г.В. Падалко визначає державне управління в якості засобу формування відповідної системи та механізмів із боку соціально орієнтованих органів державної влади. У вказаному контексті державна політика виступає в якості вектору, спрямованого на вироблення та реалізацію завдань публічного управління, «в тому числі й у сфері місцевого самоврядування щодо підтримки й розвитку територіальних громад» (Падалко, 2007: 41).

Деякі вчені розглядають державну політику в ролі провідного інституту політичної системи суспільства, «який призначений організовувати та спрямовувати спільну діяльність людей і соціальних груп» (Юридична енциклопедія, 2003).

Для усвідомлення сутності державної політики у сфері національної безпеки (кібернетичної безпеки) в умовах гібридної війни звернемося до статті 2 Закону України «Про національну безпеку», яка визначає правову основу зазначеного напрямку державної діяльності у вигляді Конституції України, коментованого та деяких інших законів України, міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, а також виданих на виконання Конституції та законів України інших нормативно-правових актів.

Так, відповідно до статті 17 Конституції України інформаційна безпека, поряд із суверенітетом та територіальною цілісністю держави, виступає пріоритетним завданням державної політики, «справою всього українського народу» (Конституція України від 28.06.1996 р.). Закон України «Про національну безпеку» у частині 1 статті 3 деталізує сутність державної політики в окресленому напрямку суспільних відносин та визначає її спрямування на захист: а) людини і громадянина – їхніх життя і гідності, конституційних прав і свобод, безпечних умов життєдіяльності; б) суспільства – його демократичних цінностей, добробуту та умов для сталого розвитку; в) держави – її конституційного ладу, суверенітету, територіальної цілісності та недоторканності; г) території, навколишнього природного середовища – від надзвичайних ситуацій.

Таким чином, захист національних інтересів у сфері кібербезпеки виступає багатофункціональним процесом, що містить цілий комплекс зазначених у вищевказаному законодавчому акті заходів.

Заслуговує на увагу висновок деяких авторів (Манилов, 1995: 16) щодо необхідності здійснення уніфікованої та виваженої державної політики у процесі реалізації органами державної влади та органами місцевого самоврядування механізму забезпечення національної безпеки (кібербезпеки). Відповідно до вказаного положення підставою реалізації державної політики у визначеній сфері суспільних відносин мають слугувати базові документи стратегічного планування, як-от Концепції, Стратегії і т.д.

Якщо й надалі притримуватися цієї логіки, виявляється, що у процесі захисту національних інтересів, під час формування державної політики в галузі національної безпеки (кібербезпеки), доцільно застосування широкого підходу, який розкриває її сучасний напрям, заснований на принципі взаємодоповнення та взаємоузгодження процесу вирішення завдань національної безпеки та активного державного соціально-економічного розвитку, що, безумовно, узгоджується із положеннями Стратегії національної безпеки України.

На підставі вищевикладеного можемо констатувати, що державна політика у сфері забезпечення національної безпеки (кібербезпеки) відноситься до вищого інтегрованого елемента внутрішньої та зовнішньої

політики України та являє собою систему цілей, а також сукупність принципів, норм, напрямків та форм діяльності органів державної влади у сфері забезпечення національної безпеки (кібербезпеки) та стійкого соціально-економічного розвитку країни.

Отже, з метою формування комплексної державної політики на сучасному етапі державотворення вважаємо за доцільне продовжити наукове системне дослідження нових викликів та загроз з огляду на їхнє триваюче збільшення в умовах гібридної війни. Для реалізації цього наукового завдання пропонуємо звернутися до положень Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 року № 96/2016.

Таким чином, слід констатувати, що Стратегія національної безпеки – це нормативно-правовий акт, який має загальнонаціональний характер та, серед іншого, визначає загрози національній безпеці (кібербезпеці) держави, першочерговою з яких у теперішніх складних для системи державного управління умовах виступає агресія РФ на території України. Її подолання, виходячи зі змісту коментованої Стратегії, не може бути реалізовано виключно зусиллями органів державної влади і потребує організації комплексної протидії. Зазначений документ націлений на підвищення якості державного управління та координацію діяльності органів державної влади, публічних та громадських організацій із захисту національних інтересів та забезпеченню державної, громадської та особистої безпеки. При цьому важливий аспект організації державного управління полягає в забезпеченні партнерських відносин держави, бізнесу та громадянського суспільства, що також є одним з основоположних принципів інформаційного суспільства.

Стратегія кібербезпеки України стала віддзеркаленням ключових положень щорічного послання Президента України до Верховної Ради України, в якому визначені такі пріоритетні напрямки в галузі внутрішньої та зовнішньої політики держави у сфері забезпечення національної безпеки України: вдосконалення політичної системи, оптимізація державного управління та місцевого самоврядування, вирішення завдань довгострокового соціально-економічного розвитку країни; покращення можливостей держави у сфері національної оборони та безпеки; розвиток виробництва та новітніх технологій; підвищення рівня та якості життя громадян (Аналітична доповідь до щорічного послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2018 році»).

Отже, організаційні заходи реалізації державної політики у сфері національної безпеки України (кібербезпеки) безпосередньо пов'язані із цілями, завданнями та принципами розвитку інформаційного суспільства у частині вдосконалення системи державного управління на основі використання інформаційних та телекомунікаційних технологій.

Разом із тим на теперішній час рівень забезпечення кібербезпеки не повною мірою відповідає потребам суспільства й держави. В умовах інформаційного суспільства загострюються протиріччя між потребою громадянського суспільства в розширенні прав і свобод щодо використання інформаційних ресурсів, з одного боку, та необхідністю забезпечення обмежень на її поширення, з іншого.

3. Проблеми правового та методологічного характеру у сфері забезпечення кібернетичної безпеки України

Удосконалення інституційного механізму кібербезпеки держави, на наш погляд, повинно бути спрямоване на вирішення проблеми, пов'язаної з декларативністю інформаційного законодавства.

Слід констатувати, що численні проблеми правового та методологічного характеру в переважній більшості випадків зумовлені недостатньою практичною спрямованістю сучасного законодавства у сфері забезпечення кібербезпеки. Зазначене твердження випливає, зокрема, з аналізу Доктрини інформаційної безпеки України, яка за окремими своїми положеннями не має прикладного значення, а також містить окремі неточності та методологічні помилки. Зокрема, у частині 1 розділу 3 Доктрини інформаційної безпеки України визначені національні інтереси України в інформаційній сфері. Звертає на себе увагу те, що в якості об'єкта вказаних суспільних відносин визначено саме інтереси, а не їх носіїв.

Так, законодавець робить акцент на життєво важливих інтересах особи (п. 1 частини 1 розділу 3) та життєво важливих інтересах суспільства і держави (п. 2 частини 1 розділу 3). Вважаємо такий підхід дискусійним, адже, по-перше, такі правові категорії, як особа, суспільство і держава, мають різне правове навантаження та обсяг компетенції у сфері забезпечення кібербезпеки. Застосування цих категорій, зміст яких залишається невизначеним, у законодавчому документі є не зовсім доречним. Наприклад, аналіз кодифікованих законодавчих актів дає підстави твердити, що до суб'єктів права відносяться переважно юридичні та фізичні особи, організації, особи без громадянства, виконавчі органи влади та органи місцевого самоврядування. Зокрема, відповідно до статті 2 Цивільного кодексу України суб'єктами цивільних відносин визнаються фізичні особи та юридичні особи, держава Україна, Автономна Республіка Крим, територіальні громади, іноземні держави та інші суб'єкти публічного права (Цивільний кодекс України : закон України від 16.01.2003 № 435-IV). Аналогічна позиція висловлена законодавцем у статті 2 Господарського кодексу України, де суб'єктами господарських відносин вважаються суб'єкти господарювання, споживачі, органи державної влади та органи місцевого самоврядування, наділені господарською компетенцією, а також громадяни, громадські та інші організації, які виступають засновниками суб'єктів господарювання чи здійснюють щодо них організаційно-господарські повноваження на основі відносин власності (Господарський кодекс України: закон України від 16.01.2003 № 436-IV). Кримінальний процесуальний кодекс у статті 3 серед суб'єктів судового прова-

дження також визначає конкретних його учасників (Кримінальний процесуальний кодекс : закон України від 13.04.2012 № 4651-VI. 14). Звертаємо увагу, що в жодному коментованому правовому акті не йдеться про інтереси осіб у якості об'єкта правовідносин, вплив правових норм здійснюється на безпосередніх учасників правових відносин. Таким чином, доцільним, на нашу думку, є віднесення до об'єктів охорони у сфері забезпечення кібербезпеки виключно носіїв суспільних інтересів, а не самі інтереси.

4. Висновки

Отже, окремі недоліки та рамковий характер Доктрини інформаційної безпеки України знижують ефективність і обмежують сферу її застосування, визначають хибний напрямок розвитку законодавства в кіберсфері та вносять плутанину в процесі його застосування.

Для належного забезпечення кібербезпеки доцільним вважаємо утворення відповідної системи правових відносин, що, у свою чергу, неможливо без перегляду категоріального апарату, доктринального і концептуального фундаменту законодавства в інформаційній сфері.

Загалом слід констатувати, що державна політика у сфері забезпечення кіберезпеки передбачає формування законодавчих основ та інституційних структур, які її забезпечують. З метою вдосконалення державної політики у вказаному напрямку державного управління і формування нової архітектури національної безпеки в умовах інформаційного суспільства доцільним вважаємо запровадження системи заходів, що включає: подолання декларативного характеру законодавства і скорочення розриву між законодавством і правозастосовною діяльністю в кіберсфері, уточнення загроз кібербезпеки України, а також утворення нових інститутів на кшталт Національного координаційного центру кібербезпеки, які визначають рамки взаємодії і правил поведінки в Інтернет-просторі.

ЛІТЕРАТУРА:

1. Гібридна війна: in verbo et in praxi : монографія / Донецький національний університет імені Василя Стуса / під заг. ред. проф. Р.О. Додонова. Вінниця : ТОВ «Нілан-ЛТД», 2017. 412 с.
2. Про національну безпеку : закон України від 21.06.2018 № 2469-VIII. *Відомості Верховної Ради*. 2018. № 31. Ст. 241.
3. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту : монографія. Київ : Видавничий дім «АртЕк», 2017. 107 с.
4. Тертичка В. Державна політика: аналіз та здійснення в Україні : монографія. Київ : Основи, 2002. 750 с.
5. Кутафин О.Е. Предмет конституционного права. Москва : Юристъ, 2001. 444 с.
6. Падалко Г.В. Функції держави у сфері місцевого самоврядування в Україні : дис... канд. юрид. наук : 12.00.02. Інститут законодавства Верховної Ради України. Київ, 2007. 224 с.
7. Юридична енциклопедія : у 6 т; редкол.: Ю.С. Шемшученко (відп. ред.) та ін. Київ : Укр. Енцикл., 2003. URL : http leksika.com.ua/19320925 (дата звернення: 30.06.2019).
8. Конституція України від 28.06.1996 р. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.
9. Манилов В.Л. Теория и практика организации системы обеспечения национальной безопасности : дис. д-ра полит. наук. Москва, 1995. 366 с.
10. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : указ Президента України від 15.03.2016 № 96/2016. *Офіційний вісник України*. 2016. № 23. Ст. 899.
11. Аналітична доповідь до щорічного послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2018 році». URL : http://www.niss.gov.ua/catalogue/33/ (дата звернення: 15.06.2019).
12. Цивільний кодекс України : закон України від 16.01.2003 № 435-IV. *Відомості Верховної Ради України*. 2003. № 40. Ст. 356.
13. Господарський кодекс України : закон України від 16.01.2003 № 436-IV. *Відомості Верховної Ради України*. 2003. № 18. Ст. 144.
14. Кримінальний процесуальний кодекс : закон України від 13.04.2012 № 4651-VI. *Відомості Верховної Ради України*. 2013. № 9-10. Ст. 88.

REFERENCES:

1. Dodonova R. O. (2017). Gibridna vijna: in verbo et in praxi [Hybrid war: in verbo et in praxi] : monograph . / Vasyl Stus Donetsk National University / Vinnytsia : Nilan LTD, 412 p.
2. Pro natsional'nu bezpeku : zakon Ukrayiny [About national security: Law of Ukraine] of 21.06.2018 № 2469-VIII. Information of the Verkhovna Rada. 2018. № 31. Art. 241.
3. Dovgan A. D., Doronin I. M. (2017). Eskalatsiya kiberzagroz natsional'nym interesam Ukrayiny ta pravovi aspekty kiberzakhystu [Escalation of cyber threats to national interests of Ukraine and legal aspects of cyber defense] : monograph . Kyiv : ArtEk Publishing House, 107 p.
4. Tertichka V. (2002). Derzhavna polityka: analiz ta zdiisnennya v Ukraine [State Policy: analysis and implementation in Ukraine] : monograph. Kyiv : Fundamentals, 750 p.
5. Kutafin O. E. (2001). Predmet konstitutsionnogo prava [The subject of constitutional law] . M. : Lawyer, 444 p.
6. Padalko G. V. (2007). Funktsii derzhavy u sferi mistsevogo samovryaduvannya v Ukraine [Functions of the state in the area of local self-government in Ukraine] : dis ... Cand. lawyer. Sciences : 12.00.02. Institute of Legislation of the Verkhovna Rada of Ukraine. Kyiv, 224 p.
7. Jurydychna entsiklopediya [Legal encyclopedia] : 6 tons; editors : yu. S. Shemshuchenko (ed.) and others. K . : Ukr. Encycl., 2003. URL : http leksika.com.ua/19320925.
8. Konstytutsiya Ukrayiny [The Constitution of Ukraine] of 28.06.1996 . Information of the Verkhovna Rada of Ukraine. 1996. № 30. Art. 141.
9. Manilov V. L. (1995). Teoriya i praktika organizatsii sistemy obespecheniya natsionalnoj bezopasnosti [Theory and practice of organization of the national security system] : diss. Dr. Polit. sciences. M ., 366 p.
10. Pro rishennya Rady natsionalnoyi bezpeky i oborony Ukrayiny vid 27 sichnya 2016 roky «Pro Strategiyu kiberbezpeky Ukrayiny» [On the decision of the National Security and Defense Council of Ukraine of January 27, 2016 «On the Cybersecurity Strategy of Ukraine»] : Presidential Decree № 96/2016 of 15.03.2016. Official Bulletin of Ukraine. 2016. № 23. Art. 899.
11. Analitychna dopovid' do shchorichnogo poslannya Prezydenta Ukrayiny do Verhovnoyi Rady Ukrayiny «Pro vnutrishne ta zovnishne stanovishe Ukrayiny v 2018 rotsi» [Analytical report on the annual message of the President of Ukraine to the Verkhovna Rada of Ukraine «On Internal and External Situation of Ukraine in 2018»] . URL : http://www.niss.gov.ua/catalogue/33/.
12. Tsivil'nij kodeks Ukrayiny [Civil Code of Ukraine] : Law of Ukraine of January 16, 2003, № 435-IV. Information of the Verkhovna Rada of Ukraine. 2003. № 40. Art. 356.
13. Gospodars'kyj kodeks Ukrayiny [Economic Code of Ukraine] : Law of Ukraine from january 16, 2003 № 436-IV. Information of the Verkhovna Rada of Ukraine. 2003. № 18. Art. 144.
14. Kriminal'nyj protsesyal'nyj kodeks [Criminal Procedure Code] : Law of Ukraine of april 13, 2012 № 4651-VI. Information of the Verkhovna Rada of Ukraine. 2013. № 9-10. Art. 88.

Стаття надійшла до редакції 24.06.2019.
The article was received 24 June 2019.