Електронне "**Державне управління: удосконалення та розвиток**"
включено до переліку наукових фахових видань України з питань державного управління
(Наказ Міністерства освіти і науки України від 22.12.2016 № 1604)
www.dy.nayka.com.ua | № 11 2018 р. | 30.11.2018

DOI: 10.32702/2307-2156-2018.11.4

УДК 351

В. В. Шпачук,
доктор наук з державного управління,
Таврійський національний університет імені В.І. Вернадського

ДЕРЖАВНЕ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ УКРАЇНИ: ПРАВОВИЙ АСПЕКТ

V. V. Shpachuk
Doctor of Science in Public Administration,
Taurida National University named after V.I. Vernadsky

STATE CYBERSECURITY MANAGEMENT OF UKRAINE: LEGAL ASPECTS

Однією з ключових проблем сучасності є проблема захисту інформації, що обробляється в інформаційно-телекомунікаційних системах, від викликів і загроз у кібернетичному просторі. В умовах глобалізації світової економіки та інформаційного обміну, глобального поширення та впровадження інформаційних технологій в усіх сферах життєдіяльності суспільства проблема захисту інформації постали перед усіма державами світу. Можливості кібернетичного простору створили фундаментальну залежність від нормального функціонування інформаційних технологій всіх сфер життєдіяльності окремих громадян, суспільства та держави: економіки, політики, сфери національної та міжнародної безпеки тощо. Така залежність стає вразливим місцем у функціонуванні систем і об'єктів критичних національних інфраструктур і дає можливість негативно налаштованим елементам і угрупованням скористатися нею для реалізації протиправних дій у кібернетичному просторі шляхом порушення цілісності, доступності й конфіденційності інформації та нанесення шкоди інформаційним ресурсам і телекомунікаційним системам.

Дослідження ж процесу становлення правової бази здійснення державного управління кібернетичною безпекою України дозволяє виявити еволюцію пріоритетів, підходів до формування засад державного управління, тенденції та закономірності державного управління кібернетичною безпекою протягом всього періоду незалежності України та на сучасному етапі розвитку. На основі ретроспективного аналізу процесу становлення правової бази державного управління кібернетичною безпекою України можуть бути встановлені напрями подальшого вдосконалення правової бази, які дозволять нейтралізувати наявні та потенційні загрози і виклики національній безпеці, запобігти проблемам у функціонуванні та розвитку національних інтересів людини, суспільства, держави.

З огляду на це, у статті представлено результати дослідження процесу становлення правової бази державного управління кібернетичною безпекою України з часу набуття Україною незалежності у 1991 році. Окремо в статті проаналізовано та виділено основні особливості законодавчих, нормативно-правових актів, концепцій та стратегій, тощо, які стосуються процесу державного управління кібернетичною безпекою України.

One of the key issues of our time is the problem of protecting information processed in information and telecommunication systems from challenges and threats in cybernetic space. In the context of the globalization of the global economy and the exchange of information, the global spread and implementation of information technologies in all spheres of society's life, the problem of information security was posed to all countries of the world. The possibilities of the cybernetic space have created a fundamental dependence on the normal functioning of information technologies in all spheres of life of individual citizens, society and the state: economics, politics, national and international security, and others like that. Such dependence becomes a vulnerable place in the functioning of systems and objects of critical national infrastructures and allows the negatively-minded elements and groups to use it for the implementation of unlawful actions in cybernetic space by violating the integrity, availability and confidentiality of information and inflicting damage on information resources and telecommunication systems.

The study of the process of establishing a legal framework for the implementation of public administration by cybernetic security of Ukraine allows us to identify the evolution of priorities, approaches to the formation of the principles of state governance, trends and patterns of state management of cybernetic security throughout the period of Ukraine's independence and at the current stage of development. On the basis of a retrospective analysis of the process of establishing a legal framework for public administration of cybernetic security in Ukraine, directions for further improvement of the legal framework that will enable to neutralize existing and potential threats and challenges to national security, prevent problems in the functioning and development of national interests of a person, society and the state can be established.

In view of this, the article presents the results of the study of the process of formation of the legal framework for state administration of cybernetic security in Ukraine since the independence of Ukraine in 1991. Separately the article analyzes and highlights the main features of legislative, normative legal acts, concepts and strategies, etc., concerning the process of public administration of cybernetic security of Ukraine.

***Ключові слова**: державне управління; кібербезпека; загроза; закон; постанова; стратегія; концепція.*

***Key words**: government; cybersecurity; threat; law; resolution; strategy; concept.*

Постановка проблеми. Швидкий розвиток інформаційних та комп’ютерних технологій, що спостерігався останні десятиріччя призвів до того, що у 21 сторіччі відмінними рисами світової економіки стали: інформатизація всіх сфер діяльності суспільства, коли майже всі сфери діяльності держави та економіки є ІТ-залежними і не можуть існувати та функціонувати без інформаційних систем; формування інформаційного суспільства, ключову роль в якому стали грати численні онлайнові соціальні мережі; розвиток фінансового сектора стало в багато залежати від надійного функціонування глобальних інформаційно-комунікаційних технологій; поява кіберпростору, яке розглядається в якості нового «домену» для проведення державної та військової політики, а також цифрової дипломатії (онлайнової зовнішньої політики).

Як зазначалось Ш. Генрі, який вважається одним з найбільш авторитетних та впливових фахівців Федерального бюро розслідуваннь (США) з питань комп'ютерної злочинності «найбільш суттєву загрозу в даний час представляють вже не «вільні молодики-хакери», а наступні три джерела кібер-атак: організовані злочинні групи, які, як правило, орієнтуються на сектор фінансових послуг і постійно нарощують кількість і різноманітність своїх атак; закордонні державні структури, які цікавляться крадіжкою даних, в тому числі інтелектуальної власності, з компаній-розробників, урядових агентств і корпорацій - військових підрядників; терористичні групи, які шукають нові способи впливу на політику держави за допомогою масштабних кібератак на критично важливі об'єкти інфраструктури».

З огляду на це сучасне державне управління з одного боку, повинно враховувати появу такого нового виду зброї як кібернетичне, яке здатне зламувати різноманітні інформаційні системи, може використовуватись під час ведення гібридних війн, чинити вплив на перебіг політичних подій, створювати загрозу національній безпеці будь-якої держави тощо. З іншого боку, кожна держава повинна мати

відповідну систему кібернетичної безпеки, засновану на відповідній нормативно-правовій базі, в якій повинні бути закладені ключові підвалини національної кібербезпеки, що б дозволяло ефективно упереджувати та протидіяти всіляким кібернетичним атакам, сприяло подальшій розбудові ефективних кіберспроможностей держави.

Аналіз останніх досліджень і публікацій. Значний внесок у дослідження різних аспектів інформаційної безпеки та її забезпечення внесли такі вітчизняні та зарубіжні науковці як М. Гуцалюк, В. Ліпкан, В. Лужецький, А. Марущак, В. Петрик та інші. Теоретико-методологічні аспекти дослідження політики інформаційної безпеки розглядаються в роботах таких дослідників як: О. Бєлов, А. Гальчинський, В. Горбулін, Е. Лисицин, А. Качинський, Г. Почепцов, О. Соснін та інших. Питанням забезпечення кібернетичної безпеки держави присвячені праці таких науковців як А. Бабенко, В. Бурячок, В. Бутузов, В. Гавловский, С. Гнатюк, В. Голубєв, Р. Лук'янчук, В. Номоконов, В. Петров, М. Погорецький, В. Шеломенцев та інші.

Мета дослідження. Метою статті є дослідження процесу становлення правової бази здійснення державного управління кібернетичною безпекою України.

Виклад основного матеріалу. На сьогодні ми маємо ситуацію, коли глобальна інформатизація активно управляє існуванням і життєдіяльністю держав світової спільноти, а інформаційні технології використовуються на самих вищих рівнях державного управління при вирішенні завдань забезпечення національної, військової, економічної безпеки тощо. Разом з тим, одним з фундаментальних наслідків глобальної інформатизації державних і військових структур стало виникнення і принципово нового середовища для співіснування та взаємодії держав – кіберпростору. При цьому, слід зважити, що кіберпростір хоча і має ознаки міжнародного, не має певних географічних ознак в загальноприйнятому у світі сенсі, характеризується відсутністю кордонів, динамікою і відносною анонімністю. Наслідком цього стало перенесення питання кібербезпеки з рівня захисту інформації на окремому об'єкті обчислювальної техніки на рівень створення єдиної системи кібербезпеки держави, як складової частини системи інформаційної та національної безпеки, що відповідає за захист не тільки інформації у вузькому сенсі цього слова, а й усього кіберпростору.

Перші концептуальні засади державного управління кібербезпекою в Україні були закладені на початку набуття Україною незалежності. Так, в ст. 7 Конституції України зазначено: забезпечення інформаційної безпеки України є однією із найважливіших функцій держави та справою всього Українського народу [1]. Зазначене формулювання свідчить про те, що: по-перше, забезпечення інформаційної безпеки є одним з пріоритетних напрямків забезпечення національної безпеки України, на одному рівні із суверенітетом, територіальною цілісністю чи економічною безпекою; по-друге, на державному рівні існує усвідомлення ролі інформаційних та кібертехнологій у сучасному світі; по-третє, на державному рівні існує усвідомлення необхідності побудови системи забезпечення кіберпезпеки та боротьби із кіберзлочинністю.

З огляду на вищевикладене, держава не просто бере на себе обов'язок здійснювати захист громадян від негативного впливу, а й делегує повноваження по протидії даному явищу громадянам. Тобто, у разі виникнення загрози кожна особа власними силами зобов'язана протидіяти кіберзлочинцям, водночас, держава забезпечує захист шляхом створення компетентних органів та прийняття необхідного законодавства.

В цей же період було прийнято ряд перших ключових законів з досліджуваного питання:

- 1992 року було прийнято Закон України «Про інформацію» № 2657-XII від 02.10.1992;

- 1994 року було прийнято Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР, у якому врегульовано відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Так, об'єктами захисту даним законом визначено інформацію, яка обробляється в системі, та програмне забезпечення, яке призначене для обробки цієї інформації [2]. Хоча, як і у попередніх випадках, мова не іде про кіберзлочинність, чи кіберзлочини у широкому розумінні, основні положення даного Закону дозволяють віднести його до переліку найважливіших інструментів національного правового регулювання питання державного управління кібербезпекою;

- Концепція (основи державної політики) національної безпеки України, схваленою постановою Верховної Ради України від 16 січня 1997 року № 3/97, яка втратила чинність одночасно із прийняттям 19 червня 2003 року Закону України «Про основи національної безпеки України».

Наступний етап активності у формуванні правових засад державного управління кібербезпекою розпочався на початку 21 сторіччя шляхом прийняття ряду важливих законів та указів Президента України:

- Указ Президента України «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні» від 31.07.2000 р. № 928/2000. Даним Указом було передбачено, що у зв'язку з прийняттям курсу розвитку мережі Інтернет в нашій державі, основними завданнями щодо цього визначено гарантування інформаційної безпеки держави та вдосконалення правового регулювання діяльності суб'єктів інформаційних відносин [3];

- Указ Президента України «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережі передачі даних» від 24.09.2001 р. № 891/2001. Даним Указом визначались завдання для органів

виконавчої влади для підвищення рівня захисту державних інформаційних ресурсів та забезпечення інформаційної безпеки держави [4];

- Указ Президента України Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України» від 6 грудня 2001 р. за № 1193/2001. Даним Указом передбачалось розроблення Концепції національної інформаційної політики та інформаційної безпеки України, здійснення заходів щодо оптимізації системи державних органів, які реалізують інформаційну політику та вжиття заходів стосовно першочергової реалізації та повноцінного фінансування найактуальніших із них та інших важливих заходів забезпечення інформаційної безпеки [5];

- Закон України «Про основи національної безпеки України» від 19.06.2003 № 964-IV, у якому окрім закріплення ряду ключових понять було визначено, що на сучасному етапі одними з основних реальних та потенційних загроз національній безпеці України, стабільності в суспільстві, в інформаційній сфері є комп'ютерна злочинність та комп'ютерний тероризм. Важливим моментом є те, що одним із основних напрямів державної політики з питань національної безпеки України визначено вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну [6].

У 2007 році було розроблено «Стратегію національної безпеки», затверджену Указом Президента України від 12 лютого 2007 року № 105. В зазначеній Стратегії передбачалась розробка та впровадження національних стандартів та технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих з відповідними європейськими стандартами, у тому числі згідно з вимогами Конвенції про кіберзлочинність [7].

У подальшому Указом Президента України від 8 червня 2012 року № 389 було затверджено нову редакцію «Стратегії національної безпеки України "Україна у світі, що змінюється", у якій було визначено нездатність держави протистояти викликам, пов'язаним із застосуванням інформаційних технологій в умовах глобалізації, насамперед кіберзагрозам [8]. Прийняття нової редакції Стратегії національної безпеки було зумовлено в основному політичними причинами, зокрема призупиненням поступу до євроатлантичної інтеграції.

Наступний етап активної нормотворчої діяльності щодо формування правових засад державного управління кібербезпекою розпочався після революції «гідності» та початку російської агресії на територію України. Так, Указом Президента України № 449/2014 від 1 червня 2014 року було уведено в дію рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України». Вказаним документом, серед іншого, передбачено (передбачалося) приведення національного законодавства у відповідність із міжнародними стандартами з питань інформаційної та кібернетичної безпеки, вдосконалення системи формування та реалізації державної політики у сфері інформаційної безпеки України тощо.

В травні 2015 року була прийнята «Стратегія національної безпеки України», в якій було визначено загрози кібербезпеці і безпеці інформаційних ресурсів та безпеці критичної інфраструктури. При цьому, до пріоритетів забезпечення кібербезпеки і безпеки інформаційних ресурсів Стратегією віднесено: розвиток інформаційної інфраструктури держави; створення системи забезпечення кібербезпеки, розвиток мережі реагування на комп'ютерні надзвичайні події (CERT); моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації; розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів; забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, відмова від програмного забезпечення, зокрема антивірусного, розробленого у Російській Федерації; реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з урахуванням практики держав-членів НАТО та ЄС; створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО, зокрема в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки.

Низка ключових доктринальних документів і підзаконних нормативно-правових актів була прийнята в 2016-2017 роках:

- «Концепція розвитку сектору безпеки і оборони України», затверджена Указом Президента України від 14.03.16 р. № 92/2016. Дана Концепція визначає, що одним із основних завдань сектору безпеки і оборони є забезпечення інформаційної та кібербезпеки, створення національної системи кібербезпеки з використанням можливостей суб'єктів сектору безпеки і оборони для ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю, розвитку мережі реагування на комп'ютерні надзвичайні події (CERT));

- «Стратегія кібербезпеки України», затверджена Указом Президента України від 15 березня 2016 року № 96/2016;

- «Стратегічний оборонний бюлетень», уведений в дію Указом Президента України від 06.06.16 р. № 240;

- «Положення про Національний координаційний центр кібербезпеки», затверджене Указом Президента України від 07.06.16 р. № 242/2016, керівником якого є секретар Ради національної безпеки і оборони України. Компетенція Національного координаційного центру кібербезпеки визначена ч. 2 ст. 5 Закону України «Про основні засади забезпечення кібербезпеки України». Зокрема Центр здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України;

- «Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави», затверджений постановою Кабінету Міністрів України від 23.08.16 р. № 563;

- «Доктрина інформаційної безпеки України», затверджена Указом Президента України від 25лютого 2017 року № 47/2017»;

- Указами Президента України від 16 січня № 8/2017 уведено в дію рішення РНБО України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури» та від 13 лютого 2017 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації».

Окремо слід виділити спеціальний законодавчий акт з питань кібербезпеки – «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року. Згідно п. 1 його Прикінцевих та перехідних положень Закон набуває чинності через 6 місяців після його опублікування. Офіційне опублікування тексту законодавчого акту відбулось у газеті "Голос України" 9 листопада 2017 року, тому він набрав чинності 9 травня 2018 року. У преамбулі Закону зазначено, що цей Закон "визначає правові та організаційні основи забезпечення захисту життєвоважливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки" [9].

У ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України», відповідно до якої до основних суб'єктів забезпечення кібербезпеки віднесено: Раду національної безпеки і оборони України, Міністерство внутрішніх справ України, Міністерство оборони України, Генеральний штаб Збройних Сил України, Службу безпеки України, Державну службу спеціального зв'язку та захисту інформації України, розвідувальні органи, тощо. Згідно з ч. 4 статті 5 цього Закону суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є:

1) міністерства та інші центральні органи виконавчої влади;

2) місцеві державні адміністрації;

3) органи місцевого самоврядування;

4) правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності;

5) Збройні Сили України, інші військові формування, утворені відповідно до закону;

6) Національний банк України;

7) підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури;

8) суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

У межах своїъ компетенцій суб'єкти забезпечення кібербезпеки:

1) здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях;

2) здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;

3) здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз;

4) розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту;

5) забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління;

6) здійснюють інші заходи із забезпечення розвитку та безпеки кіберпростору [9].

Висновки. Формування та розвиток правової бази з питання державного управління кібербезпекою України відбувалось хвилеобразно з піковою активністю, що мала місце в певні періоди. Воно не було системним і залежало від вподобань та пріоритетів політичної сили, що перебувала у влади, водночас здійснювалось з урахуванням документів міжнародно-правового характеру у розрізі резолюцій Генеральної асамблеї ООН щодо культури кібербезпеки у сучасних умовах, директив Європейського Союзу тощо. Агресія проти України у 2014 році, що відбувалася з активним використанням бойових дій проти нашої держави у кіберпросторі, а також посилення загальносвітових загроз кібербезпеці зумовили прискорення формування спеціального законодавства з даного питання. Найбільш активно зазначений процес відбувався останні три роки.

Переважна більшість з законодавчих та нормативно-правових актів встановлює загальні засади державного управління, державної політики і визначає окремі підходи до унормування питань забезпечення

кібербезпеки. Водночас, деякі заходи та стратегічні підходи не повною мірою базуються на науковому підґрунті, що неодмінно призведе до виникнення спірних питань стосовно правової регламентації.

Список використаних джерел.

1. Конституція України від 28.06.1996 № 254к/96-ВР. [Електронний ресурс]. – Режим доступу : http://zakon1.rada.gov.ua/laws/show/ 254к/96-вр вр (дата звернення: 22.10.2018).
2. Про захист інформації в інформаційно-телекомунікаційних системах. Закон України від 05.07.1994 № 80/94-ВР. Відомості Верховної Ради України (ВВР). 1994. № 31. ст.286.
3. Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні // Урядовий кур'єр від 08.08.2000. URL zakon.rada.gov.ua (дата звернення: 23.09.2018).
4. Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних. Указ Президента України від 24.09.2001 № 891/2001 // Урядовий кур'єр від 03.10.2001. № 179. URL zakon.rada.gov.ua (дата звернення: 01.10.2018).
5. Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року "Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України». Указ президента України від 06.12.2001 № 1193/2001. Урядовий кур'єр від 18.12.2001. № 235.
6. Про основи національної безпеки України. Закон України від 19.06.2003 № 964-IV. Відомості Верховної Ради України (ВВР). 2003. № 39. ст.351.
7. Стратегія національної безпеки України: затверджена Указом Президента України від 12.02.2007 № 105. Офіційний вісник України. 2007. 23.02.2007. No 11. – С. 7. Ст. 389.
8. Про рішення Ради національної безпеки і оборони України від 8 червня 2012 року "Про нову редакцію Стратегії національної безпеки України": Указ Президента України від 08.06.2012 № 389. Офіційний вісник України. 2012. 22.06.2012. № 45. С. 104. Ст. 1749.
9. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII / Верховна Рада України. Відомості Верховної Ради. 2017. № 45. Ст.403.

Referenses.

1. The Verkhovna Rada of Ukraine (1996), "The Constitution of Ukraine", available at: http://zakon5.rada.gov.ua/laws/show/en/254%D0%BA/96-D0%B2% D1%80 (Accessed 22 October 2018).
2. The Verkhovna Rada of Ukraine (1996), The Law of Ukraine "On the protection of information in information and telecommunication systems", Vidomosti Verkhovnoyi Rady Ukrainy, vol. 31, p. 286.
3. The Verkhovna Rada of Ukraine (2000), The Law of Ukraine "About measures on the development of the national component of the global Internet information network and ensuring wide access to this network in Ukraine", available at: zakon.rada.gov.ua (Accessed 23 September 2018).
4. President of Ukraine (2001), The Decree "Some measures to protect state information resources in data transmission networks", available at: zakon.rada.gov.ua (Accessed 10 September 2018).
5. President of Ukraine (2001), The Decree "On the decision of the Council of National Security and Defense of Ukraine of October 31, 2001 "On Measures to Improve State Information Policy and Ensuring Information Security of Ukraine", Uryadovyy kur'yer, vol. 235, p. 1865.
6. The Verkhovna Rada of Ukraine (2003), The Law of Ukraine "On the Fundamentals of National Security of Ukraine", Vidomosti Verkhovnoyi Rady Ukrainy, vol. 39, p. 351.
7. President of Ukraine (2007), The Decree "Strategy of National Security of Ukraine", Ofitsijnyj visnyk Ukrainy, vol. 11, p. 7.
8. President of Ukraine (2012), The Decree "On the decision of the National Security and Defense Council of Ukraine dated June 8, 2012 "On the new edition of the Strategy of National Security of Ukraine", Ofitsijnyj visnyk Ukrainy, vol. 45, p. 104.
9. The Verkhovna Rada of Ukraine (2017), The Law of Ukraine "On the main principles of ensuring cyber security of Ukraine", Vidomosti Verkhovnoyi Rady Ukrainy, vol. 45, p. 403.

Стаття надійшла до редакції 20.11.2018 р.