УДК 351.86:659.3. 4:004](477)

О. В. Коваленко,
аспірант кафедри глобалістики, євроінтеграції та управління національною безпекою,
Національна академія державного управління при Президентові України
ORCID ID: 0000-0001-8350-6442

DOI: 10.32702/2306-6814.2020.17—18.149

РОЗБУДОВА СИСТЕМИ КІБЕРБЕЗПЕКИ ІСПАНІЇ: УРОКИ ДЛЯ УКРАЇНИ

O. Kovalenko,
Postgraduate student of the Department of European integration and globalization and management of national security, National Academy of Public Administration under the President of Ukraine

DEVELOPMENT OF CYBERSECURITY SPAIN: LESSONS FOR UKRAINE

Метою статті є узагальнення та систематизація досвіду Республіки Іспанії у сфері забезпечення кібербезпеки та оцінка можливості його використання у вітчизняній державно-управлінській практиці.

Для вирішення завдань дослідження нами використовувалися: методи аналізу і синтезу, інституціональний та системно-ситуаційний підходи.

З'ясовано, що керівництво Іспанії досягнуло значних результатів у розбудові національної системи кібербезпеки, а саме: а) реалізовано перспективну модель кібербезпеки на основі задіяння компонентів забезпечення кібербезпеки визначених в керівних документах НАТО і ЄС; б) сформовано інституційне середовище кібербезпеки, яке структурно містить правовий, організаційний, самоорганізаційний, соціокультурний, когнітивний компоненти.

Обгрунтовано доцільність використання у практиці публічного управління у сфері забезпечення кібербезпеки України досвіду Іспанії щодо: визначення перспективної моделі кібербезпеки; формування інституційного середовища кібербезпеки з урахуванням вимог зовнішнього та внутрішнього безпекового середовища до національної системи кібербезпеки.

The purpose of the article is to generalize and systematize the experience of the Republic of Spain in the field of cybersecurity and assess the possibility of its use in domestic public administration practice.

To solve the research problems we used: methods of analysis and synthesis — to understand the problems of cybersecurity; institutional approach — to study foreign experience in the field of cybersecurity; system-situational approach — to assess the possibilities of implementing the positive experience of the Republic of Spain in the domestic public administration practice.

An analysis of the National Cyber Security Strategy of Spain, which identifies the basics of protection of cyberspace of the state, in particular the implementation of coordinated and coordinated actions aimed at preventing and combating identified cyber threats and eliminating the consequences of their implementation.

It was found that the Spanish leadership, building a national cybersecurity system in the context of NATO and EU security policy priorities, has achieved significant results in this specific area, namely: a) implemented a promising model of cybersecurity based on five components of cybersecurity: legal framework in the field of guaranteeing the state's cybersecurity; high operational capabilities of the state cybersecurity forces; an effective system of public-private partnership in the field of cybersecurity; an effective planning system in the field of cybersecurity in various sectors; appropriate level of education in the field of cybersecurity; b) the institutional environment of cybersecurity is formed, which structurally contains legal, organizational, self-organizational, socio-cultural, cognitive components.

The expediency of using in the practice of public administration in the field of cyber security of Ukraine the experience of Spain on: definition of a promising model of cybersecurity; formation of the institutional environment of cybersecurity taking into account the requirements of the external and internal security environment to the national cybersecurity system.

Ключові слова: інституційне середовище безпеки, національна безпека, публічне управління національною безпекою, національна система кібербезпеки, розбудова національної системи кібербезпеки.

Keywords: institutional security environment, national security, public management of national security, national cybersecurity system, development of national cybersecurity system.

ПОСТАНОВКА ПРОБЛЕМИ

Трансформації безпекового простору в умовах глобалізації характеризуються тим, що надзвичайні події в кіберпросторі стають все частішими та масштабнішими. За таких умов, що склалися на перший план виходять питання забезпечення кіберстійкості та захисту критичної інфраструктури від кіберінцидентів. Для вирішення цих питань країни-члени НАТО та ЄС, а також міжна-

родні організації реалізовують політику кібербезпеки, яка спрямована на запобігання, мінімізацію та своєчасне і адекватне реагування на кіберінциденти.

Ця обставина і визначає зв'язок загальної проблеми з найбільш важливими науковими та практичними завданнями дослідження проблем теорії та практики адаптації досвіду країн-членів НАТО та ЄС щодо забезпечення кібербезпеки для потреб України.

На підставі аналізу актуальних досліджень і наукових публікацій можна дійти висновку, що проблеми забезпечення кібербезпеки країн-членів НАТО та ЄС привертають увагу вітчизняних дослідників. Для вивчення цієї проблематики велике значення мають наукові праці вітчизняних науковців, зокрема: В Ліпкана та І. Діордіци [1; 2], М. Кольцова та Є. Аушева [3], О. Лалак [4], В. Чигринського [5] та ін. Аналіз вказаних наукових праць дозволяє констатувати, що, попри наявність загальновизнаних принципів та підходів щодо забезпечення кібербезпеки в країнах-членах ЄС та НАТО, кожна національна система кібербезпеки є по суті унікальною і неминуче несе на собі відбиток національної специфіки, яку слід враховувати при використанні зарубіжного досвіду у вітчизняній практиці публічного управління у сфері забезпечення кібербезпеки.

ВИДІЛЕННЯ НЕ ВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ

Утім, результатів системного вивчення досвіду Республіки Іспанії щодо забезпечення кібербезпеки в науковій літературі автор не зустрічав.

З огляду на це, метою статті є узагальнення та систематизація досвіду Республіки Іспанії у сфері забезпечення кібербезпеки та оцінка можливості його використання у вітчизняній державно-управлінській практиці.

Для вирішення завдань дослідження нами використовувалися: методи аналізу і синтезу — для осмислення проблем забезпечення кібербезпеки; інституціональний підхід — для вивчення зарубіжного досвіду у сфері забезпечення кібербезпеки; системно-ситуаційний підхід — для оцінки можливостей впровадження позитивного досвіду Республіки Іспанії у вітчизняну державно-управлінську практику.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

У рамках інституціонального підходу вітчизняний дослідник В.І. Абрамов визначає основні компоненти інституційного середовища безпеки [6, с. 237—242]:

1) нормативно-правовий компонент функціональне призначення якого полягає у правовому регулюванні відносин і взаємодій в системі безпеки, а також у визначенні пріоритетів, цілей і напрямів політики безпеки, структуризації інституційного простору сфери безпеки;

2) організаційний компонент функціональне призначення якого полягає в організації управлінська діяльність органів публічної влади щодо забезпечення національної безпеки, а також діяльності органів судової влади щодо контролю за виконанням норм у сфері національної безпеки;

3) самоорганізаційний компонент функціональне призначення якого полягає в інституалізації та реалізації інтересів громадських, благодійних та релігійних організацій, професійних спілок та їх об'єднань, творчих спілок, асоціацій, організацій роботодавців, недержавних ЗМІ, неурядових аналітичних центрів, непідприємницьких товариств та установ, які легалізовані відповідно до національного законодавства;

4) соціокультурний компонент функціональне призначення якого полягає у формуванні культури національної безпеки та організаційної культури в публічному управлінні;

5) когнітивний компонент функціональне призначення якого полягає у розвитку системи наукових знань у сфері безпекознавства, публічного управління і адміністрування. Зокрема Міжнародна торгівельна асоціація BSA (Business SoV ware Allience), яка була створена у 1988 р. виробниками програмного забезпечення розробила для країн-членів ЄС матрицю оцінки кібербезпеки [3, с. 16]. Ця матриця дозволяє оцінити рівень забезпечення кібербезпеки за наступними критеріями:

наявність та якість нормативно-правової бази в галузі гарантування кібербезпеки держави;

операційні можливості сил забезпечення кібербезпеки держави;

державно-приватне партнерство у сфері забезпечення кібербезпеки;

наявність окремих планів для окремих секторів забезпечення кібербезпеки;

освіта у сфері кібербезпеки.

Задіяння всіх п'яти компонентів забезпечення кібербезпеки є пріоритетом розвитку національних систем кібербезпеки країн-членів НАТО і ЄС.

Розглянемо питання формування нормативно-правової компоненти інституційного середовища кібербезпеки Іспанії. Так, у 2010 р. країнами-членами НАТО була прийнята Стратегічна концепція НАТО [7], а також країнами-членами ЄС Європейська стратегія безпеки [8] в яких значна увага приділялася питанням виявлення і захисту країн-членів НАТО і ЄС від кібератак.

На початку 2013 р. ЄС ухвалив Стратегію кібербезпеки, яка мала на меті гарантування відкритого, надійного і безпечного кіберпростору. З метою досягнення вказаної мети в цій Стратегії були передбачені заходи за такими напрямами [3, с. 10]:

1. Забезпечення кіберстійкості.

2. Боротьба із кіберзлочинністю.

3. Розробка політики кібероборони, яка має узгоджуватися із Спільною політикою безпеки і оборони.

4. Розвиток виробничих і технологічних ресурсів у інтересах забезпечення кібербезпеки ЄС.

5. Розробка міжнародної політики кібербезпеки узгодженої з інтересами ЄС у цій сфері.

Варто зазначити, що після оприлюднення Стратегії кібербезпеки ЄС було розпочато роботу над директивою щодо її реалізації з урахуванням вимог Стратегії Єдиного Цифрового Ринку та Європейського Порядку Денного з питань безпеки.

На виконання вимог Стратегії кібербезпеки ЄС 5 грудня 2013 року Рада національної безпеки Іспанії схвалила Стратегію національної кібербезпеки [9]. Цей

документ є правовою основою для діяльності Уряду Іспанії в контексті виконання положень Стратегії національної безпеки (2013 р.) [10] щодо захисту кіберпростору держави, зокрема щодо реалізації узгоджених і злагоджених дій спрямованих на профілактику та протидію виявленим кіберзагрозам та ліквідацію наслідків їх реалізації.

Стратегія національної кібербезпеки складається з 5 розділів [9].

У розділі I містяться:

загальні характеристики кіберпростору;

можливості, які надає кіберпростір;

наслідки залежності від нього з точки зору безпеки.

У розділі також акцентовано увагу на такій сучасній тенденції розвитку інформаційного суспільства в Іспанії, як зростання кількості ризиків та загроз кібербезпеці в умовах інформатизації суспільства. При цьому джерелами загроз кібербезпеці Іспанії визначено: іноземні держави, організована злочинність, терористичні організації, хакери. Водночас причинам загроз кібербезпеці визначено: технічні причини, природні явища, суспільні явища (конфлікти). Ризикам та загрозами кібербезпеці Іспанії визначено: хакерство, тероризм, саботаж, злочинність, шпигунство; внутрішні загрози.

Розділ II визначає місію системи кібербезпеки Іспанії та основні принципи її функціонування. Зокрема місією визначено запровадження загальних правил безпечного використання кіберпростору за допомогою комплексного бачення, яке передбачає координацію дій органів державної влади, приватного сектору та громадян, а також міжнародні ініціативи з дотриманням національного і міжнародного права, інших національних та міжнародних стратегічних документів.

Керівними принципами функціонування національної системи кібербезпеки визначено:

національне лідерство і координація зусиль;

спільна відповідальність;

пропорційність, раціональність і ефективність;

міжнародне співробітництво.

Ці принципи підкреслюють необхідне планування розвитку національної системи кібербезпеки з особливим акцентом на захисті національних цінностей визначених у Конституції Іспанії (1978 р.) [11].

У розділі III Стратегії детально визначено цілі та завдання національної системи кібербезпеки. Національними цілями у сфері забезпечення кібербезпеки Іспанії визначено:

гарантування безпечного використання інформаційних і телекомунікаційних систем;

зміцнення спроможностей держави щодо виявлення, аналізу, оцінки рівня загроз кібербезпеці;

попередження та захист від загроз кібербезпеці;

своєчасне та адекватне реагування на кібератаки;

відновлення інформаційних і телекомунікаційних систем після кібератак.

Визначені національні цілі у сфері кібербезпеки досягаються в ході реалізації державної політика кібербезпеки Іспанії.

Завданнями системи кібербезпеки Іспанії є:

1) для органів державної влади — гарантувати кібербезпеку та стійкість інформаційних та телекомунікаційних систем, які ними використовуються;

2) для підприємств і об'єктів критичної інфраструктури — підвищити рівень кібербезпеки і стійкості мереж та інформаційних систем, які використовуються в бізнес-секторі в цілому і, зокрема, операторами критичної інфраструктури;

3) у судовій та поліцейській сфері — розширення можливостей з профілактики, виявлення, реагування та координації діяльності у сфері боротьби з тероризмом і злочинністю в кіберпросторі;

4) у сфері сенсибілізації (підвищення чутливості) — ознайомлення громадян, фахівців компаній та органів державної влади з ризиками та загрозами кібербезпеці;

5) у сфері освіти — здобуття знань, формування навичок, досвіду і технологічних можливостей, яких потребує Іспанія для досягнення всіх національних цілей у сфері забезпечення кібербезпеки;

6) у рамках міжнародного співробітництва — сприяння підвищенню рівня кібербезпеки шляхом розвитку скоординованої політики кібербезпеки в ЄС та міжнародних організаціях, а також шляхом співпраці в галузі освіти з іншими державами.

У розділі IV визначено 8 основних напрямів досягнення національних цілей у сфері забезпечення кібербезпеки:

попередження і виявлення кіберзагроз, своєчасне та адекватне реагування на них і ліквідації наслідків їх реалізації;

гарантування безпеки інформаційних і телекомунікаційних систем органів державної влади;

гарантування безпека інформаційних і телекомунікаційних систем на об'єктах критичної інфраструктури;

боротьба із кібертероризмом та кіберзлочинністю;

гарантування безпеки і стійкості ІКТ приватного сектора;

здобуття релевантних знань та формування навичок у фахівців у сфері кібербезпеки, а також впровадження інноваційних технологій у практику забезпечення кібербезпеки;

формування культури кібербезпеки;

виконання міжнародних зобов'язань у сфері забезпечення кібербезпеки.

У розділі V визначено місце системи кібербезпеки в системі національної безпеки Іспанії, а також визначається її інституційна структура.

Організаційний компонент інституційного середовища кібербезпеки Іспанії представлено трьома органами, що безпосередньо опікуються питаннями кібербезпеки, а саме:

Радою національної безпеки;

Спеціалізованим комітетом з кібербезпеки, який надає допомогу Раді національної безпеки у контексті реалізації політики національної безпеки у сфері кібербезпеки, а також координує співпрацю між органами державної влади і приватним сектором;

Ситуативним спеціалізованим комітетом, який за допомогою Ситуативного центру Департаменту національної безпеки Секретаріату Глави Уряду Іспанії управляє кризовими ситуаціями в кіберпросторі, які за своїми масштабами і складністю не можуть бути вирішені

звичайними методами реагування на загрози кібербезпеці [9];

Національним Центром із захисту критичної інфраструктури (CNPIC). Цей Центр відповідає:

за інформаційну безпеку та кібербезпеку;

за поширення інформації щодо кіберзагроз та кіберінцидентів;

забезпечує координацію та співпрацю між різними секторами економіки та між державними та приватними інституціями.

Одним із завдань CNPIC є створення робочих Груп, які розробляють секторальні плани забезпечення кібербезпеки [3, с. 17].

Організаційний компонент інституційного середовища кібербезпеки Іспанії представлено також Національним центром розвідки Іспанії (НЦР), що опосередковано опікується питаннями кібербезпеки. НЦР є основним державним відомством, яке здійснює розвідувальну й контррозвідувальну діяльність на території Іспанії та за її межами, а також координує діяльність розвідувальних органів інших відомств (міністерства оборони, міністерства внутрішніх справ, міністерства фінансів). Основне завдання НЦР — це надання уряду необхідної інформації для виявлення та запобігання будь-яких загроз чи небезпеки для незалежності та територіальної цілісності Іспанії, її національних інтересів.

Відповідно до Закону №11/2002 "Про діяльність Національного центру розвідки", найвищим координуючим та контролюючим органом за діяльністю розвідувальних структур є Урядова комісія з питань розвідки, яка керує організацією взаємодії між усіма розвідувальними службами держави. Крім того, Комісія надає пропозиції Главі Уряду щодо основних завдань НЦР на рік, особливо тих, які будуть включені до Розвідувальної Директиви, здійснює контроль за виконанням НЦР головних завдань, керує взаємодією НЦР з інформаційними службами, органами безпеки держави, військовими та цивільними установами [12].

Комісія, яку очолює Перший заступник Глави Уряду, складається з міністрів закордонних справ, оборони, внутрішніх справ, економіки, а також керівника Кабінету Глави Уряду, державного секретаря з питань національної безпеки, державного секретаря — директора НЦР. На засіданнях комісії можуть бути присутніми особи вищого керівного та виконавчого складу органів державної влади, яких комісія вважає за необхідне запросити.

В Іспанії також огранізовано "гарячу лінію" функціональне призначення якої полягає:

у захисті дітей від шкідливого контенту;

у підвищенні обізнаності щодо ризиків кібербепеці;

у налагодженні співпраці між різними стейкголдерами з питань забезпечення кібербезпеки [3, с. 17].

Чинною Стратегією кібербезпеки Іспанії [9] передбачено формування та функціонування:

самоорганізаційного компоненту інституційного середовища кібербезпеки, в рамках якого здійснюється державно-приватне партнерство у сфері забезпечення кібербезпеки;

соціокультурного компоненту інституційного середовища кібербезпеки, в рамках якого здійснюється формування культури кібербезпеки.

Когнітивний компонент інституційного середовища кібербезпеки Іспанії представлено Вищим центром досліджень національної оборони [13] та Іспанським інститутом стратегічних досліджень [14].

Системно-ситуаційний підхід щодо оцінки можливостей запровадження зарубіжного досвіду забезпечення національної безпеки, що запропонований в [15] дозволив нам здійснити оцінку можливостей впровадження позитивного досвіду Республіки Іспанії у вітчизняну державно-управлінську практику у цій специфічній сфері. На нашу думку, досвід Іспанії у сфері забезпечення кібербезпеки може бути використаний щодо:

а) визначення перспективної моделі кібербезпеки на основі задіяння всіх п'яти компонентів забезпечення кібербезпеки, а саме:

досконала нормативно-правова база в галузі гарантування кібербезпеки держави;

високі операційні можливості сил забезпечення кібербезпеки держави;

ефективна система державно-приватного партнерства у сфері забезпечення кібербезпеки;

ефективна система планування у сфері забезпечення кібербезпеки у різних секторах;

належний рівень освіти у сфері кібербезпеки.

б) формування інституційного середовища кібербезпеки з урахуванням вимог як зовнішнього так і внутрішнього безпекового середовища до національної системи кібербезпеки.

ВИСНОВКИ

1. З'ясовано, що керівництво Іспанії здійснюючи розбудову національної системи кібербезпеки в контексті пріоритетів політики безпеки НАТО і ЄС досягло значних результатів у цій специфічній сфері, а саме:

а) реалізовано перспективну модель кібербезпеки на основі задіяння п'яти компонентів забезпечення кібербезпеки: досконалої нормативно-правової бази в галузі гарантування кібербезпеки держави; високих операційних можливостей сил забезпечення кібербезпеки держави; ефективної системи державно-приватного партнерства у сфері забезпечення кібербезпеки; ефективної системи планування у сфері забезпечення кібербезпеки у різних секторах; належного рівня освіти у сфері кібербезпеки.

б) сформовано інституційне середовище кібербезпеки, яке структурно містить правовий, організаційний, самоорганізаційний, соціокультурний, когнітивний компоненти.

2. На нашу думку, Україні на сучасному етапі розбудови національної системи кібербезпеки в умовах європейської та євроатлантичної інтеграції, доцільно використати досвід Іспанії щодо:

а) визначення перспективної моделі кібербезпеки;

б) формування інституційного середовища кібербезпеки з урахуванням вимог зовнішнього та внутрішнього безпекового середовища до національної системи кібербезпеки.

Перспективним напрямом подальших досліджень вбачається в подальшому узагальненні і систематизації досвіду країн-членів НАТО і ЄС щодо забезпечення кібербезпеки та оцінці можливостей щодо його використання в Україні.

Література:

1. Ліпкан В., Діордіца І. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України. Підприємництво, господарство і право. 2017. № 5. С. 174—180.

2. Діордіца І. Система забезпечення кібербезпеки: сутність та призначення. Підприємництво, господарство і право. 2017. № 7. С. 109—116.

3. Кольцов М., Аушев Є. Пропозиції до політики щодо реформування сфери кібербезпеки в Україні. URL: https://parlament.org.ua/wp-content/uploads/2017/10/Policy-Paper_Kiberbezpeka-1-1.pdf (дата звернення: 12.06.2020).

4. Лалак О.А. Виклики і ризики кібербезпеки: досвід України та Польщі. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/download/3001/2692 (дата звернення: 12.06.2020).

5. Чигринський В. А. Політико-правове проектування та державне конструювання системи забезпечення національної безпеки Іспанії: уроки для України. Державне управління: удосконалення та розвиток. 2020. № 6. — URL: http://www.dy.nayka.com.ua/?op=1&z=1692 (дата звернення: 12.09.2020).

6. Шляхи удосконалення системи державного управління забезпеченням національної безпеки України: монографія / В.І. Абрамов, О.Г. Бортнікова, М.М. Шевченко та ін.; за ред. Г.П. Ситника, В.І. Абрамова. Київ: МАЙСТЕР КНИГ, 2012. 536 с.

7. Декларація саміту НАТО в Страсбурзі. URL: http://www.nato.int (дата звернення: 15.06.2020).

8. Безопасная Европа в мире, который должен стать лучше. Европейская стратегия безопасности. URL: http://www.consilium.europa.eu/uedocs/cmsUpload/031208ESSIIRU.pdf (дата звернення: 15.06.2020).

9. Estrategia de Ciberseguridad Nacional. URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/ES_NCSS.pdf (дата звернення 21.04.2015).

10. Estrategia de Seguridad Nacional. URL: www.lamoncloa.gob.es/NR/rdonlyres/OBB61AA9 (дата звернення 21.04.2015).

11. Constitucion de Espana de 1978. URL: www.congreso.es/consti/ (дата звернення 22.04.2015).

12. Ley 11/2002, de 6 de mayo reguladora del Centro Nacional de Inteligencia URL: http://www.cni.es/comun/recursos/descargas/LEY_11-2002_de_6_-de_mayo_.pdf (дата звернення 22.04.2015).

13. Centro Superior de Estudios de la Defensa Nacional URL: http://www.defensa.gob.es/ceseden/ (дата звернення 22.04.2015).

14. Instituto Espanol de Estudios Estrategicos URL: http://www.ieee.es/ (дата звернення 22.04.2015).

15. Шевченко М.М. Методологія компаративного аналізу систем забезпечення національної безпеки. Збірник наукових праць Національної академії державного управління при Президентові України / за заг. ред. Ю.В. Ковбасюка. К.: НАДУ, 2015. Вип. 1. С. 5—16.

References:

1. Lipkan, V. and Diorditsa, I. (2017), "National cybersecurity system as an integral part of the national security system of Ukraine", Pidpryiemnytstvo, hospodarstvo i pravo, vol. 5, pp. 174—180.

2. Diorditsa, I. (2017), "Cybersecurity system: essence and purpose", Pidpryiemnytstvo, hospodarstvo i pravo, vol. 7, pp. 109—116.

3. Kol'tsov, M. and Aushev, Ye. (2017), "Proposals for a policy on cybersecurity reform in Ukraine", available at: https://parlament.org.ua/wp-content/uploads/2017/10/Policy-Paper_Kiberbezpeka-1-1.pdf (Accessed 12 Sept 2020).

4. Lalak, O.A. (2017), "Challenges and risks of cybersecurity: the experience of Ukraine and Poland", available at: http://journals.iir.kiev.ua/index.php/pol_n/article/download/3001/2692 (Accessed 12 Sept 2020).

5. Chyhrynskyi, V. (2020), "Political and legal design and state construction of spain's national security system: lessons for Ukraine", Derzhavne upravlinnya: udoskonalennya ta rozvytok, [Online], vol. 6, available at: http://www.dy.nayka.com.ua/?op=1&z=1692 (Accessed 12 Sep 2020). DOI: 10.32702/2307-2156-2020.6.100

6. Abramov, V.I. Bortnikova, O.H. and Shevchenko, M.M. (2012), Shliakhy udoskonalennia systemy derzhavnoho upravlinnia zabezpechenniam natsional'noi bezpeky Ukrainy [Ways to improve the system of public administration of national security of Ukraine], MAJSTER KNYH, Kyiv, Ukraine.

7. NATO (2009), "Declaration of the NATO Summit in Strasbourg", available at: http://www.nato.int (Accessed 12 Sept 2020).

8. European Council (2020), "A secure Europe in a better world. European security strategy", available at: http://www.consilium.europa.eu/uedocs/cmsUpload/031208ESSIIRU.pdf (Accessed 12 Sept 2020).

9. Presidente del Gobierno (2013), "Estrategia de Ciberseguridad Nacional", available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/ES_NCSS.pdf (Accessed 12 Sept 2020).

10. Ministerio de Defensa de Espana (2017), "Estrategia de Seguridad Nacional", available at: www.lamoncloa.gob.es/NR/rdonlyres/OBB61AA9 (Accessed 12 Sept 2020).

11. Constitucion de Espana (1978), available at: www.congreso.es/consti/ (Accessed 12 Sept 2020).

12. Centro Nacional de Inteligencia (2002), "Ley 11/2002, de 6 de mayo reguladora del Centro Nacional de Inteligencia", available at: http://www.cni.es/comun/recursos/descargas/LEY_11-2002_de_6_de_mayo_.pdf (Accessed 12 Sept 2020).

13. Centro Superior de Estudios de la Defensa Nacional (2020), available at: http://www.defensa.gob.es/ceseden/ (Accessed 12 Sept 2020).

14. Instituto Espanol de Estudios Estrategicos (2020), available at: http://www.ieee.es/ (Accessed 12 Sept 2020).

15. Shevchenko, M.M. (2015), "Methodology of comparative analysis of national security systems", Zbirnyk naukovykh prats' Natsional'noi akademii derzhavnoho upravlinnia pry Prezydentovi Ukrainy, vol. 1, pp. 5—16.

Стаття надійшла до редакції 16.09.2020 р.