РОЗДІЛ 4
ДЕРЖАВНЕ УПРАВЛІННЯ У СФЕРІ ДЕРЖАВНОЇ БЕЗПЕКИ ТА ОХОРОНИ ГРОМАДСЬКОГО ПОРЯДКУ

УДК 351.88
DOI https://doi.org/10.51547/ppp.dp.ua/2021.6.9

Годлевська Валентина Юріївна,
доктор історичних наук, професор,
професор кафедри публічного управління та адміністрування
Вінницького державного педагогічного університету
імені М. Коцюбинського
ORCID ID: 0000-0001-8115-5116

Кононенко Валерій Васильович,
доктор історичних наук, професор,
завідувач кафедри публічного управління та адміністрування
Вінницького державного педагогічного університету
імені М. Коцюбинського
ORCID ID: 0000-0001-5177-2885

КІБЕРБЕЗПЕКА: ДЕРЖАВНЕ УПРАВЛІННЯ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ІСПАНІЇ

CYBER SECURITY: PUBLIC ADMINISTRATION IN THE FIELD OF NATIONAL SECURITY OF SPAIN

У статті висвітлено особливості державного управління у сфері кібербезпеки Іспанії. Із початком пандемії у світі значно збільшилася кількість кібератак як на державні, так і на приватні структури. Тому гарантування і забезпечення безпеки у кіберпросторі стало одним із стратегічних пріоритетів розвинених країн через його безпосередній вплив на національну безпеку, на конкурентоспроможність компаній і на процвітання суспільства загалом. Значних успіхів у розробленні власної системи Національної кібербезпеки досягла Іспанія. Ця система, очолювана головою уряду, сформована із трьох органів: Ради національної безпеки (Consejo de Seguridad Nacional) як делегованої комісії уряду з національної безпеки; Національної ради із кібербезпеки (Consejo Nacional de Ciberseguridad), що є складовою частиною Ради національної безпеки, допомагаючи голові уряду спрямовувати і координувати політику національної безпеки у сфері інформаційної безпеки, а також сприяючи координації, співпраці між державними адміністраціями, між ними та приватним сектором; Ситуаційного комітету (El Comité de Situación), який за підтримки Департаменту внутрішньої безпеки підтримує управління кризовими ситуаціями у будь-якій сфері, які через свою масштабність перевищують можливості застосування звичайних механізмів. Окреме місце у забезпеченні безпеки у кіберпросторі Іспанії посідає Національний криптологічний центр, що підпорядковується Національному розвідувальному центру при Міністерстві оборони. Починаючи із 2013 року, в Іспанії один раз у декілька років ухвалюється Національна стратегія із кібербезпеки. Досвід цієї держави засвідчив успішність заходів, що впроваджуються. Підтвердженням цього є те, що глобальний індекс кібербезпеки, підготовлений Міжнародним союзом телекомунікацій Організації Об'єднаних Націй, ставить Іспанію на 7-ме місце у світі.

Ключові слова: *Іспанія, державне управління, національна безпека, інформатизація, кіберпростір, кібербезпека, кібератаки.*

The article reflects the features of public administration in the field of cybersecurity in Spain. Since the beginning of the pandemic, the number of cyberattacks both against government agencies and private ones has significantly increased in the world. Therefore, guaranteeing and ensuring security in cyberspace has become one of the strategic priorities of developed countries through its direct impact on national security, the competitiveness of companies and the prosperity of society as a whole. Spain has made significant progress in developing its own national cybersecurity system. Its national security system, headed by the head of government, is formed of three bodies: the National Security Council (Consejo de Seguridad Nacional)

as a delegated government commission on national security; The National Council for Cybersecurity (Consejo Nacional de Ciberseguridad), which is part of the National Security Council, helps the head of government to direct and coordinate national security policy in the field of cybersecurity, and also promotes coordination, cooperation between public administrations and between public administrations and the private sector; The Situation Committee (El Comité de Situación), with the support of the Department of Homeland Security, supports crisis management in any area, which, due to its scale, exceeds the capabilities of conventional mechanisms. A separate place in ensuring security in cyberspace in Spain is occupied by the National Cryptological Center, which is under the jurisdiction of the National Intelligence Center under the Ministry of Defense. Since 2013, Spain has adopted a National Cybersecurity Strategy every few years. The experience of this state has shown the success of the measures being taken, which is confirmed by the fact that the global cybersecurity index prepared by the United Nations International Telecommunications Union puts Spain in 7th place in the world.

Key words: *Spain, public administration, national security, informatization, cyberspace, cybersecurity, cyber attacks.*

Глобальна інформатизація у сучасному світі активно управляє існуванням та життєдіяльністю держав світової спільноти. Інформаційні технології застосовуються під час вирішення завдань забезпечення національної, військової, економічної безпеки тощо. Водночас одним із фундаментальних наслідків глобальної інформатизації стало виникнення принципово нового середовища протиборства конкуруючих держав – кіберпростору. Під цим поняттям розуміють сукупність взаємопов'язаних інформаційних ресурсів, програмного забезпечення, баз і банків даних, які обробляються у комп'ютерних мережах та у пов'язаній із ними інфраструктурі разом із об'єктами, що підпадають під їхній контроль та управління. Під час формування глобального кіберпростору відбувається конвергенція військових та цивільних комп'ютерних технологій, у провідних зарубіжних державах інтенсивно розробляються нові засоби та методи активного впливу на інформаційну інфраструктуру потенційних противників, створюються різні спеціалізовані кібернетичні центри і підрозділи командування, основним завданням яких є захист державних інформаційних інфраструктур.

Кіберсвіт вимагає постійного пристосування до технологічного розвитку та все більшої складності кібератак. Адаптація до цих реалій передбачає покращення можливостей запобігання та розроблення більш ефективних заходів реагування на атаки. Це також вимагає більшої координації та співпраці, з одного боку, на національному рівні, між усіма рівнями державної адміністрації та приватними компаніями і структурами, а з іншого – на міжнародному рівні.

Із початком пандемії у світі значно збільшилася кількість кібератак як на державні, так і на приватні структури. Таке збільшення пов'язане зі створенням «ідеального сценарію» для кіберзлочинців, якому сприяло не лише зменшення інвестицій у безпеку внаслідок кризи, але і тому, що відбувався поспішний процес «цифровізації», який більшість компаній, особливо МСП, змушена була поспішно впроваджувати задля адаптації до технічних вимог дистанційної роботи.

Значних успіхів у розробленні власної системи Національної кібербезпеки досягла Іспанія. Глобальний індекс кібербезпеки (GCI), підготовлений Міжнародним союзом телекомунікацій Організації Об'єднаних Націй, ставить Іспанію на 7-ме місце у світі (попереду лише Сполучене Королівство, США, Франція, Литва, Естонія і Сінгапур) [1, p. 5]. Досвід цієї країни є цікавим для пізнання та аналізу.

Кібербезпека є новим витком інформаційної безпеки, а кіберпростір окремих країн і світу загалом через певну новизну активно досліджується.

Джерельною базою статті стало іспанське законодавство, що регулює державне управління у сфері кібербезпеки, а також матеріали іспанської преси.

Аналізуючи науковий доробок іспанських дослідників, варто виокремити колективну монографію «Необхідність усвідомлення національної кібербезпеки. Кіберзахист: пріоритетний виклик». Автори (Таррео Хільгадо Х. Т., Ролдан Тудела Х. М., Муньос Луіс Х., Акоста Пастор О., де Рохас Діас Е. С.) зосередили увагу на трактуванні понять «тотальна війна», «асиметрична війна», «кібервійна»; на проблемі транскордонних загроз, їхніх основних видів, «кіберзахисту» в оборонній політиці та позиціях щодо міжнародного співробітництва; на висвітленні питань пристосованості користувачів, установ і компаній до мінливих обставин кіберпростору [2]. Особливості державного управління у сфері кібербезпеки в Іспанії знаходять віддзеркалення у наукових публікаціях Балєстероса Мартіна М., Фернандеса Дельгадо Л., Пеня Муньоса Х., Рего М., Артега Мартіна Ф. та інших [1; 3; 4; 5; 6].

Наукова цінність цієї статті полягає в тому, що вперше в українській науці зроблено спробу висвітлити процес становлення і функціонування державного управління у сфері кібербезпеки Іспанії.

В Іспанії із початку пандемії було зареєстровано понад 150 тисяч кібератак [7]. Одна із найпотужніших із них сталась у березні 2021 року на Державну службу зайнятості Іспанії. Метою

кібератаки, на думку іспанців, була «дискредитація не тільки державної установи, але і самої іспанської держави, а також поява невдоволення громадськості через скасування тисячі призначень по всій Іспанії та параліч оброблення даних про допомогу із безробіття, особливо під час кризи» [8]. Хвиля кібератак на сайти Національного інституту статистики (INE) та щонайменше чотирьох міністерств (освіти, економіки, промисловості та юстиції) відбулась у квітні 2021 року [9; 10].

Система національної безпеки Іспанії, яку очолює голова уряду, складається із трьох органів: Ради національної безпеки (Consejo de Seguridad Nacional) як делегованої комісії уряду з національної безпеки; Національної ради із кібербезпеки (Consejo Nacional de Ciberseguridad) та Ситуаційного комітету (El Comité de Situación).

Цю систему доповнюють Постійна комісія з кібербезпеки (La Comisión Permanente de Ciberseguridad); компетентні державні органи та Група реагування на інциденти комп'ютерної безпеки (Computer Security Incident Response Team); Національний форум із кібербезпеки (Foro Nacional de Ciberseguridad) як елемент державно-приватного співробітництва [11, p. 43440].

Одним зі структурних елементів Ради національної безпеки (РНБ) Іспанії є Національна рада із кібербезпеки, яка є складовою частиною Ради національної безпеки, що допомагає голові уряду спрямовувати та координувати політику національної безпеки у сфері кібербезпеки, а також сприяє координації, співпраці та відносинам співпраці між державними адміністраціями, між ними і приватним сектором відповідно до закону «Про Уряд» (1997) [12, p. 35085]. Національна рада із кібербезпеки, очолювана держсекретарем, директором Національного розвідувального центру та директором Національного криптологічного центру, створена Угодою Ради національної безпеки від 5 грудня 2013 року [13]. Склад цієї Ради відображає спектр сфер діяльності департаментів, органів та відомств державного управління, які мають компетенцію у питаннях кібербезпеки, для координації тих дій, які потрібно вирішувати спільно задля підвищення рівня безпеки. У виконанні своїх функцій Національна рада з кібербезпеки підтримується Департаментом національної безпеки (Departamento de Seguridad Nacional).

На Національну раду з кібербезпеки покладені такі функції:

– підтримання рішень Ради національної безпеки з питань кібербезпеки шляхом аналізу, вивчення і пропозицій ініціатив як на національному, так і на міжнародному рівнях;

– зміцнення відносин координації, взаємодії та співпраці між різними державними адміністраціями, які мають компетенцію, пов'язану зі сферою кібербезпеки, а також між державним і приватним секторами;

– сприяння розробленню нормативних пропозицій у сфері кібербезпеки для розгляду РНБ;

– надання підтримки Раді національній безпеки у виконанні нею функції із перевірки ступеня відповідності Стратегії національної безпеки щодо кібербезпеки і сприяння її перегляду;

– перевірка ступеня відповідності Національній стратегії кібербезпеки та звітування перед РНБ;

– здійснення оцінки ризиків і загроз, аналіз можливих кризових сценаріїв, вивчення їхньої можливої еволюції, підготовка та оновлення планів реагування і формулювання рекомендацій щодо проведення навчань із кризового управління у сфері кібербезпеки, оцінка результатів їх виконання;

– сприяння доступності наявних ресурсів, проведення досліджень, аналіз можливостей державних адміністрацій розробляти ефективні заходи реагування відповідно до наявних засобів, які мають бути виконані (у координації із компетентними органами та відповідно до компетенції різних державних адміністрацій, залучених у сферу кібербезпеки);

– сприяння оперативній координації між компетентними органами та органами влади, коли цього вимагають ситуації, що впливають на кібербезпеку, та коли Спеціалізований ситуаційний комітет не в змозі діяти.

Рада збирається за ініціативою свого очільника щонайменше кожні два місяці або стільки разів, скільки він уважає за потрібне, враховуючи обставини, що впливають на кібербезпеку.

Із метою спрямування і координації дій із управління кризовими ситуаціями у грудні 2013 року був створений Ситуаційний комітет [13], який за підтримки Департаменту внутрішньої безпеки підтримує управління кризовими ситуаціями у будь-якій сфері, які через свою масштабність перевищують можливості реагування звичайних механізмів, покращує координацію між різними державними адміністраціями, сприяє швидкості та гнучкості у реагуванні на ці ситуації. Комітет має універсальний характер для всієї системи національної безпеки [11, p. 43450]. Він регулює роботу Спеціалізованого ситуаційного комітету (відповідна Постанова РНБ від 22 січня 2018 р.) [14].

Із січня 2019 року щомісячно проводяться конференції Комітету, на яких розглядаються актуальні питання національної безпеки, а також питання, спрямовані на зміцнення системи націо-

нальної безпеки та потенціалу реальної підтримки органів влади у кризових ситуаціях. У них беруть участь представники міністерств та організацій, які входять до складу Ситуаційного комітету. Департамент внутрішньої безпеки як постійний робочий орган РНБ координує ці зустрічі для виконання поставлених перед ним завдань щодо підтримання у системі задіяних постійних механізмів зв'язку.

Вперше Ситуаційний комітет було залучено під час управління надзвичайною ситуацією у галузі охорони здоров'я через пандемію COVID-19 улітку 2020 року відповідно до закону «Про національну безпеку» [15].

З метою сприяння міжвідомчій координації на оперативному рівні у сфері інформаційної безпеки була створена Постійна комісія з кібербезпеки, очолювана Департаментом національної безпеки. Вона надає допомогу Національній раді з кібербезпеки в аспектах, пов'язаних із технічною та оперативною оцінкою ризиків і загроз для безпеки ІТ систем. Комісія складається з органів та агенцій, представлених у Національному центрі координації рятувальників (CNCS) із оперативними обов'язками. Це орган, відповідальний за надання допомоги щодо аспектів, пов'язаних із технічною та операційною оцінкою ризиків і загроз інформаційній безпеці.

Діяльність Комісії є частиною процедури антикризового управління у сфері кібербезпеки. Зазначена процедура встановлює її функції, спрямовані на виявлення та оцінку ризиків і загроз; спрощення процесу прийняття рішень і забезпечення оптимальної та скоординованої реакції державних органів. Окрім того, вона містить різні рівні активації системи національної безпеки та інструкції із управління публічною комунікацією.

Стратегічну та інституційну основу кібербезпеки доповнюють компетентні органи державної влади з питань безпеки мереж та інформаційних систем, національні Групи реагування на інциденти комп'ютерної безпеки (CSIRT), включені до національного законодавства. Національні CSIRT у співпраці з автономними і приватними CSIRT сприяють реалізації ініціатив, спрямованих на досягнення цілей національної стратегії.

У 2020 році був створений Національний форум із кібербезпеки з метою просування культури кібербезпеки, надання підтримки промисловості, проведення досліджень, а також сприяння навчанню шляхом державно-приватного співробітництва під егідою Ради національної безпеки.

У 2013 році була затверджена перша в історії Іспанії Національна стратегія кібербезпеки (ENCS). У документі визначено керівні принципи і загальні напрямки дій для подолання проблеми, пов'язаної із вразливістю кіберпростору для країни. У 2017 році її змінила нова стратегія, а 30 квітня 2019 року була затверджена нині діюча Національна стратегія кібербезпеки, яка встановила п'ять цілей і сім напрямків дій, поділених на 65 заходів задля їх досягнення. Щороку складається звіт для визначення ступеня реалізації. Національна стратегія кібербезпеки є документом, який відображає необхідність покращення ІКТ-безпеки в Іспанії, детально описує цілі та заходи для їх досягнення.

З огляду на загальні цілі та напрями діяльності, встановлені для їх досягнення, документ сформовано із п'яти розділів. Перший розділ під назвою «Кіберпростір за межами глобального спільного простору» містить огляд сфери кібербезпеки. У другому розділі «Загрози та виклики у кіберпросторі» визначаються основні загрози кіберпростору, їхні різновиди. У третьому розділі визначено мету, принципи і завдання кібербезпеки. Наступний розділ присвячений таким напрямкам дій та основним заходам: зміцненню потенціалу протистояння загроз у кіберпросторі; гарантуванню безпеки і стійкості стратегічних активів Іспанії; посиленню спроможності розслідувати та переслідувати кіберзлочини, гарантувати безпеку громадян, захист прав і свобод у кіберпросторі; сприянню безпеці кіберпростору на міжнародній арені, сприяючи відкритому, безпечному та надійному кіберпростору на підтримку національних інтересів тощо. У п'ятому розділі під назвою «Кібербезпека у системі національної безпеки» визначено структуру кібербезпеки Іспанії [11, p. 43437].

Окреме місце у забезпеченні безпеки у кіберпросторі Іспанії посідає Національний криптологічний центр, який підпорядковується Національному розвідувальному центру при Міністерстві оборони.

Основна інформація про особливості функціонування центру міститься у відповідних законодавчих актах та постановах. Зокрема, закон від 6 травня 2020 року, що регулює функціонування Національного розвідувального центру, покладає на нього виконання функцій, пов'язаних із безпекою інформаційних технологій (стаття 4.e) та захистом інформації (стаття 4.f). Водночас на його директора покладено відповідальність за керівництво Національним криптологічним центром (стаття 9.2.f) [16, p. 16441].

Зазначений центр було створено у 2002 році, а його діяльність регулюється Королівським указом від 12 березня 2004 року [17]. Із моменту

створення його робота була спрямована на зниження ризиків і загроз у кіберпросторі, використання безпечних засобів і систем (він є органом із сертифікації), на сприяння навчанню, координації та комунікації між усіма залученими агентами, збереження секретної і конфіденційної інформації. Національний криптологічний центр також відіграє центральну роль у розробленні та впровадженні Системи національної безпеки (ENS) і Національної стратегії кібербезпеки.

Інформаційну безпеку нині вважають питанням національної безпеки, фундаментальною віссю суспільства та його економічних систем, тому протягом останніх двох десятиліть кібербезпека стала одним із пріоритетних питань керівництва іспанської держави. Це спричинило створення при Міністерстві оборони та Раді національної безпеки низки відповідних структур, які забезпечують нормальне функціонування інформаційного простору державних і приватних установ Іспанії, намагаються своєчасно відстежувати кіберзагрози та адекватно реагувати на кібератаки, застосовуючи сучасні методи і технології. Починаючи із 2013 року, один раз на декілька років ухвалюється Національна стратегія кібербезпеки, яка дозволяє формулювати цілі та розробляти заходи задля досягнення і підтримання високого рівня безпеки державних інформаційних систем та мереж, оскільки природа, тип і дії кібератак постійно змінюються, а заходи безпеки повинні постійно оновлюватися, щоб бути ефективними.

СПИСОК ЛІТЕРАТУРИ:

1. Ballesteros Martín M. Á. El ciberespacio lleva años consolidándose como un entorno de alta relevancia económica y social, pero también de inseguridad. Actuarios. 2021. № 48. P. 4–8. Режим доступу: https://www.actuarios.org/wp-content/uploads/2021/03/Actuarios-48-web-low.pdf

2. Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario. Ministerio de Defensa, Instituto Español de Estudios Estratégicos, 2013. 337 p. Режим доступу: https://publicaciones.defensa.gob.es/necesidad-de-una-conciencia-nacional-de-ciberseguridad-la-ciberdefensa-un-reto-prioritario-n-137-libros-papel.html

3. Fernández Delgado L. España y la ciberseguridad: hora de remangarse. Economía industrial, 2018. P. 27–36.

4. Peña Muñoz J. de la. Ciberseguridad: España no invierte. Revista SIC: ciberseguridad, seguridad de la información y privacidad. 2016. Vol. 25. № 122. P. 6.

5. Rego M. Aprovechar el talento que hay en España sobre ciberseguridad. Byte España. 2015. № 224. P. 58–59.

6. Arteaga Martín F . Ciberseguridad en España: ¿problema u oportunidad? Política exterior. 2015. Vol. 29. № 163. 2015. P. 148–156.

7. Moreno Rosalina. En España se han registrado más de 150.000 ciberataques desde el inicio de la pandemia. El Confilegal. Режим доступу: https://confilegal.com/20211021-270846/

8. Un ciberataque deja sin servicio la web y el sistema informático del SEPE. El Confidencial. Режим доступу: https://www.elconfidencial.com/tecnologia/2021-03-09/ciberataque-sepe-cae-web-ataque-informatico-sin-servicio_2983887/

9. Otto C., M. A. Méndez, Ignacio Cembrero. Una oleada de ciberataques tumba las webs del INE, Justicia, Economía y más ministerios. El Confidencial. Режим доступу: https://www.elconfidencial.com/tecnologia/2021-04-23/ciberataques-ccn-cni-justicia-ine-interior_3047336/

10. Méndez Manuel A. C. Otto. Así se descubrió el ciberataque al Gobierno que tiene en vilo al CNI y a la Guardia Civil. El Confidencial. Режим доступу: https://www.elconfidencial.com/tecnologia/2021-04-24/ciberataque-cobalt-strike-ine-ministerios-ransomware_3048224/

11. Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional. *Boletín Oficial del Estado*. 2019. № 103. 30 de abril. P. 43437–43455.

12. Ley 50/1997, de 27 de noviembre, del Gobierno. *Boletín Oficial del Estado*. 1997. № 285, 28 de noviembre. P. 35082–35088.

13. La Estrategia de Ciberseguridad Nacional. 2013. Gobierno de Espana Precidensia del Gobierno. Режим доступу: https://www.dsn.gob.es/estrategias-publicaciones/estrategias/estrategia-ciberseguridad-nacional

14. Orden PRA/32/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Comité Especializado de Situación. Boletín Oficial del Estado. 2018. № 20. 23 de enero. P. 8179–8185.

15. Ruiz Enebral A. El Gobierno prepara el primer ejercicio de gestión de crisis de Seguridad Nacional. ECD Confidencial Digital. Режим доступу: https://www.elconfidencialdigital.com/articulo/seguridad/gobierno-prepara-primer-ejercicio-gestion-crisis-seguridad-nacional/20200828134032157212.html?__cf_chl_tk=T.agiL_1UcTvrRxUN6_vLExezmiRgI.QkfpmDgtGfA0-1637501400-0-gaNycGzNBtE

16. Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia. Boletín Oficial del Estado. 2002. № 109. P. 16440–16444.

17. Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional. Boletín Oficial del Estado. 2004. № 68. P. 12203–12204.