Анастасія Хмель, к. і. н.
Дмитро Біляєв
Чорноморський національний університет імені Петра Могили, Україна

ПОРІВНЯННЯ КІБЕРБЕЗПЕКОВИХ МОЖЛИВОСТЕЙ ІСПАНІЇ ТА ІТАЛІЇ НА СУЧАСНОМУ ЕТАПІ

Anastasiia Khmel, PhD in World History
Dmytro Bilyayev
Petro Mohyla Black Sea National University, Ukraine

COMPARISON OF THE CYBER SECURITY CAPACITIES OF SPAIN AND ITALY AT THE PRESENT STAGE

The article deals with the cyber security issues of Italy and Spain based on sources of information on this topic, especially the reports of the International Telecommunication Union and Potomac Institute for Policy Studies. Cyber security threats are becoming more dangerous with every year.

The authors also came to the conclusion that the general cyber security policy of the European Union and its institutions is positively affecting the described countries and the development of their cyber security capacities. It is noticeable from the analysis that Spain has better organizational possibilities, legal measures and capacity building characteristics, while Italy has more points in the technical measures and cooperation sections. The cybersecurity of the mentioned countries requires more projects aimed at the international cooperation, training of the future cyber security specialists and development of the new innovational good practices for strengthening the cyber security sphere. It is emphasized in the article that nowadays Spain and Italy have been challenged by the variety of fake news.

Keywords: cyber security, cyber space, security issues, Spain, Italy, EU.

Постановка проблеми Базуючись на доповідях європейських експертів які стверджують що до 2020 р. кількість пристроїв, які будуть обмінюватись даними користувачів зросте майже до 12 млрд. і людство буде ще більше залучене до сфери інформації, постає нагальна необхідність захисту та регулювання кіберпростору, як одного із найперспективніших та вельми вразливих напрямків. Якісний захист і регулювання кіберпростору буде визначати кількість даних, якими обмінюються користувачі і буде впливати на загальний розвиток ЄС та його учасників в подальші роки[1].

З одного боку, безпека Італії та Іспанії в ці роки перевірялась багатьма випробуваннями, такими як нелегальна міграція, нелегальна торгівля зброєю, торгівля наркотиками, торгівля людьми, тероризм, внутрішня нестабільність (зокрема, прояви сепаратизму в Каталоні). З іншого боку, необхідність вивчення можливостей кібербезпеки обох країн продиктована подіями в Європі останнім часом: збільшення кількості інформаційних атак, скандалами щодо зміни результатів виборів та референдумів третіми країнами, крадіжки персональних та секретних даних з засобів, що належать урядовим органам держав ЄС.

Окремим яскравим прикладом того, як треті країни можуть використовувати одне явище в суспільстві фальшуючи дані про нього одразу у двох площинах, є події в Каталонії від осені

[1] Global Cybersecurity Index, year: 2017 (International Telecommunication Union). *The Official website of the International Telecommunication Union.* <http://handle.itu.int/11.1002/pub/80f875fa-en> (2018, березень, 29).

2017 р. і до сьогодні. Для Іспанії цей приклад став надто вадливим і показовим порушення її кібербезпеки. Так, у жовтні голова Міноборони Іспанії Марія Долорес де Коспедаль зробила заяву, що є докази того, як РФ разом із Венесуелою впливали на розвиток подій в Каталонії, розгойдуючи ситуацію. Тоді ж представник делегації Іспанії в НАТО Рікардо Тарно заявив про наявність російської руки у Каталонському питанні. Але це тільки перша площина питання (докази дійсно є). Друга площина – стосується подій після референдуму, коли каталонці вже проголосували за незалежність. Так, іспанські ЗМІ наполягають, що дії іспанського уряду по врегулюванню ситуації в Каталонії, негативно і почастково, вириваючи окремі елементи з контексту, висвітлювалися вже поміченими у роздмухуванні подій в Каталонії соціальними мережами та каналами ЗМІ, формуючи образ центрального іспанського уряду негативно, часто перекручуючи факти[1].

За наведених фактів, описаних вище, питання кібербезпеки Італії та Іспанії є вельми актуальним та важливим у сучасній Європі.

Метою статті є визначення та порівняння кібербезпекових можливостей Іспанії та Італії на сучасному етапі.

Виходячи з мети роботи можна визначити такі **завдання**: визначити стан розробки теми науковцями на даному етапі розвитку науки; виділити оціночні критерії, за якими експерти порівнюють кібербезпекові можливості Іспанії та Італії; виокремити та проаналізувати відповідні механізми та ініціативи Іспанії та Італії у сфері кіберпростору; аналіз фактів і прикладів вразливості кібербезпекового простору Іспанії та Італії.

Методологія. Для опрацювання джерельної бази дослідження автори послуговувалися методами пошуку джерел (евристична метода) та систематизації матеріалу (за допомогою методів аналізу, синтезу та системного). В процесі виконання дослідження автори використовували як загальнонаукові методи (порівняння, співставлення, узагальнення, конкретизація) так і спеціально-наукові політологічні, до яких можна віднести контент-аналіз (який особливо допоміг при аналізі документальної бази дослідження а також звітів та досліджень у сфері кіберпростору). Такий набір методів а також використання основних імператив наукового дослідження: об'єктивність, точність, істинність висновків, дало можливість здійснити комплексний та міждисциплінарний виклад проблеми.

Ступінь наукової розробки теми. Оскільки автори статті досліджували стан кіберпростору Італії та Іспанії на сучасному етапі, то тема виглядає надто специфічною і досліджень не так вже й багато. Але якщо звернути увагу на те, які дослідники працювали над звітом щодо стану кіберпростору з Міжнародного союзу електрозв'язку, то варто назвати такі прізвища: М. Мінгес, Шеріф Хасем (Єгипет), М. Сейсана і Х. Норлен (дослідники від Європейської Комісії) та інші. І щодо самої доповіді від 2017 р., яку вони підготували від ЄС, то зазначається, що в Європі рівень захищеності кіберпростору, його правове та технічне регулювання знаходиться на дуже високому рівні, в той час як в Північній та Південній Америці та Африці, ситуація, що складається навколо кіберпростору, може характеризуватися експертами як проблематична, як така, що потребує більшого залучення та підтримки[2]. Італія та Іспанія є представниками південної частини ЄС і не потрапляють за звітами до найбільш захищених країн (в інформаційній сфері), але в той же час за різними критеріями захищеності знаходяться у різних групах. Відтак оскільки саме аспект стану захищеності Італії та Іспанії є недостатньо висвітленим, це робить тему актуальною та свідчить про прогалини у ступені наукової розробки теми.

Виклад основного матеріалу. Характерними для останніх років для Європи стали більш комплексні кібератаки на користувачів, що відбуваються через зараження шкідливим програмним забезпеченням шляхом надсилання листів. За даними 2017 р. наслідки такого зараження були найсильнішими за останні п'ять років і порівняно з 2015 р. зловмисники, які заражали комп'ютери втричі збільшили викуп за розблокування програмного забезпечення[3].

[1] La trama rusa empleó redes chavistas para agravar la crisis catalana. *Página Oficial. El Pais.* <https://politica.elpais.com/politica/2017/11/10/actualidad/1510341089_316043.html> (2018, березень, 31).
[2] Global Cybersecurity Index, year: 2017 (International Telecommunication Union). *The Official website of the International Telecommunication Union*. <http://handle.itu.int/11.1002/pub/80f875fa-en> (2018, березень, 29).
[3] Global Cybersecurity Index, year: 2017 (International Telecommunication Union). *The Official website of the International Telecommunication Union*. <http://handle.itu.int/11.1002/pub/80f875fa-en> (2018, березень, 29).

У зв'язку зі збільшенням кількості скандалів щодо зміни результатів виборів та референдумів третіми країнами, Італія як і решта членів Європейського Союзу намагається усунути від себе проблему втручання третіх країн у вибори на різних рівнях.

Вибори в Італії до сенату 2018 р. пройшли за неприємних інцидентів, пов'язаних із втручанням в діяльність інформаційних засобів, які належать урядовим органам держав ЄС та крадіжку цінної інформації та персональних даних. В січні місяці в мережі Facebook з'явилася інформація про те, що окремий портал даної мережі буде допомагати об'єктивному висвітленню виборів 2018 р. до сенату Італії та сприяти у протидії фейковим новинам, а також зменшенню рівня втручання іноземних країн до італійських виборів. Фейкові новини, зокрема ті що направлені на маніпулюваннями настроїв виборців (на зміну настроїв, активність/пасивність виборців, підтримку), формуючись на основі дезінформації соціальних медіа та стрічки міжнародних новин, сприяють непрозорій політичній кампанії і наносять шкоду тій державі проти якої були задіяні, на користь країни, яка створює, фінансує, підтримує таку компанію[1].

В Італії найбільш неоднозначні партії: «Рух 5 зірок» та «Ліга Півночі» зустрічаються відкритого та неофіційно з представниками інших країн, також представники цих партій активно діють у соціальних мережах, просуваючи популістські заклики. Перша створена була нещодавно (2009 р.), але дуже швидко набула популярності і підтримки серед населення. Вибори в Італії в 2018 р. відбулися і на разі не має повідомлень про викрадення або псування електронної інформації пов'язаної з результатами виборів, хоча деякі видання наголошують на тому що атака на державні установи не припинялася. Результати виборів підтвердили, що вплив соціальних медіа та засобів масової інформації в Інтернеті суттєво зріс та продовжує бути одним з найголовніших факторів, який може вплинути на незалежні результати виборів.

Повертаючись до подій 2017 р., одною з найсерйозніших загроз був вірус-шахрай WANNACRY, за ним відбулись атаки аналогічних вірусів. Італія також підпала під дії кібератак, деякі державні органи та електронні засоби були атаковані. Італія другою після України потрапила під вплив вірусу Petya, який був запущений злодіями на державні установи, фірми та підприємства[2]. Негативні результати цього вірусу відчула на собі й Іспанія (були атаковані її конгломерат Mondelez та юридична фірма DLA Piper).

Країни Південної Європи пройшли еволюційний шлях дослідження стану своєї кібербезпеки, приведення своїх правових, організаційних та інших сфер, що регламентують кіберпростір, до міжнародних стандартів. Базуючись на п'ятьох формотворчих критеріях, які складають глобальний індекс кібербезпеки: правовому, технічному, організаційному критерії створених потужностей і критерії проведеного співробітництва формується глобальний індекс кібербезпеки, який підкріплюється 25 оціночними питаннями що включаються до нього[3].

Найвищий рівень кібербезпеки мають ті країни, які мають найбільш комплексний інструментарій задля регулювання та організації безпеки кіберпростору. Це можуть бути або країни, які поставили собі це за більш важливу мету і ті, які виділяють на це чималі кошти.

Для того аби максимально розширено показати стан кібербезпеки окремих країн, проводиться вивчення безпеки кіберпростору країн регіону, їх порівняння а також співвідношення цілей із визначеними заздалегідь критеріями оцінки. Далі порівнюються попередні дані з наявними сучасними даними для верифікації правильності оцінки кібербезпеки цих країн. Наявні дані можуть підтверджуватись через додаткові перевірки[4].

ЄС як організація має дуже високий показник кібербезпеки у світі за усіма п'ятьма критеріями кібербезпеки. Окремо трійку лідерів ЄС з дотримання високих показників кібербезпеки на сьогоднішній час займають: Естонія, Франція та Норвегія. Італія та Іспанія не входять до трійки

[1] Negri, G. Facebook to monitor Italian election as EU debates Russian fake news. *The European Security Journal.* <https://www.esjnews.com/facebook-italy-russia-fake-news> (2018, березень, 29).
[2] Henley, J., Solon, O. 'Petya' ransomware attack strikes companies across Europe and US. The Guardian <https://www.theguardian.com/world/2017/jun/27/petya-ransomware-attack-strikes-companies-across-europe> (2018, березень, 29).
[3] Global Cybersecurity Index, year: 2017 (International Telecommunication Union). *The Official website of the International Telecommunication Union.* <http://handle.itu.int/11.1002/pub/80f875fa-en> (2018, березень, 29).
[4] Global Cybersecurity Index, year: 2017 (International Telecommunication Union). *The Official website of the International Telecommunication Union.* <http://handle.itu.int/11.1002/pub/80f875fa-en> (2018, березень, 29).

лідерів кібербезпекового простору серед країн ЄС. У загальному рейтингу оцінки кібербезпеки Іспанія випереджає Італію обіймаючи 19 позицію, в той час як друга знаходиться на 31 позиції[1].

Порівнюючи глобальний індекс кібербезпеки цих двох країн можна вказати на те, що обидві країни мають абсолютно різні загальні показники в п'яти оціночних категоріях, що свідчить про різне залучення до процесів захисту та організацією кібербезпекових заходів.

За класифікацією експертної доповіді Італія входить до групи, що має менший рівень злочинності ніж група лідерів з кібербезпеки, але вищий рівень ніж у країн, що входять до групи країн, які впроваджують заходи покращення кібербезпекового простору. Посідаючи місце у групі країн з середніми результатами, Італія демонструє високі показники безпеки у деяких оціночних питаннях із 25 загальних, але не всі цілісні показники у п'ятьох категоріях індексу є високими[2].

Порівнюючи країни у всіх п'яти категоріях, почнемо із правових заходів. Правове забезпечення країн знаходяться на різних рівнях. Іспанія в усіх чотирьох категоріях: кримінальне право та кібербезпекове право, кібербезпекова підготовка, а також у загальному індексі правових заходів отримала найвищі оцінки. Італія лише в сфері кібербезпекового права має найвищі оцінки а решта правових заходів знаходиться на найнижчому рівні[3].

Основними документами, які розроблені для регулювання правової сфери Італії є Стратегія кібербезпеки ЄС від 2013 р., Директива ЄС з питань безпеки та мережевої інформації від 2016 р. а також своя Національна стратегія кібербезпеки, яка була опублікована в 2013 р. Остання повністю розкриває цілі та методи, якими може користуватися кабінет міністрів, державні та недержавні установи задля формування безпечного кіберпростору[4].

Іспанія у сфері кібербезпеки опікується наступними документами: Стратегія національної кібербезпеки (2013 р.)[5] та Стратегія національної безпеки (2017 р.)[6]. Основна відмінність від попередньої Стратегії національної безпеки від 2013 р. полягає в тому, що ключовим питанням є боротьба з дезінформацією. Вважається, що це дуже символічно, що документ від 2017 р. з'явився за кілька днів до офіційного початку виборчої кампанії в Каталонії. Автори нової Стратегії національної безпеки посилаються на тріумф пост-правди: явище, в якому об'єктивна думка посідає друге місце у формуванні громадської думки, надаючи фундаментальну роль емоціям. В документі робиться наголос, що у світі шириться гібридна війна, і сьогодні неможливо розглядати спроби впливу на громадську совість як одноразову дію. Втручання у вибори через соціальні мережі та ЗМІ поєднується з кібер-атаками, економічним тиском та використанням традиційних сил. Наслідки цієї гібридної війни призвели до перемоги Д. Трампа на американських виборах і до «Brexit»[7]. І звичайно, Іспанія має дотримуватися директив ЄС, зокрема тієї, про яку зазначено вище.

Наступна сфера в якій є показники обох держав – це технічні можливості для організації кібербезпеки. В цій категорії у обох країн дуже високі показники в технічному забезпеченні. Іспанія має середню оцінку, а Італія має найвищу оцінку. В двох країнах створені національні команди які займаються відповідним реагуванням на інциденти у кіберпросторі та відновленням функціонування ураженого інформаційного середовища[8].

---

[1] Global Cybersecurity Index, year: 2017 (International Telecommunication Union). *The Official website of the International Telecommunication Union.* <http://handle.itu.int/11.1002/pub/80f875fa-en> (2018, березень, 29).
[2] Global Cybersecurity Index, year: 2017 (International Telecommunication Union). *The Official website of the International Telecommunication Union.* <http://handle.itu.int/11.1002/pub/80f875fa-en> (2018, березень, 29).
[3] Global Cybersecurity Index, year: 2017 (International Telecommunication Union). *The Official website of the International Telecommunication Union.* <http://handle.itu.int/11.1002/pub/80f875fa-en> (2018, березень, 29).
[4] Hathaway, M., Demchak, C., Kerben, J., McArdle, J., Spidalieri, F. Italy Cyber Readiness at a Glance. The Potomac Institute for Policy Studies. < www.potomacinstitute.org/images/CRI/PIPS_CRI_Italy.pdf> (2018, березень, 29).
[5] Estrategia de ciberseguridad nacional (2013). *Sitio oficial del Departamento de Seguridad Nacional.* <http://www.cnpic.es/Biblioteca/Legislacion/Generico/20131205_ESTRATEGIA_DE_CIBERSEGURIDAD_NACIONAL.pdf> (2018, березень, 31).
[6] Estrategia de seguridad nacional (2017). *Sitio oficial del Departamento de Seguridad Nacional.* <http://www.dsn.gob.es/sites/dsn/files/Estrategia_de_Seguridad_Nacional_ESN%20Final.pdf > (2018, березень, 31).
[7] La seguridad de ciberespacio como garantía de la integridad de España, por María García López. *Página Oficial del Diariocritico. Sábado 9 de diciembre de 2017.* <https://www.diariocritico.com/opinion/maria-garcia-lopez/seguridad-de-ciberespacio> (2018, березень, 31)
[8] Global Cybersecurity Index, year: 2017 (International Telecommunication Union). *The Official website of the International Telecommunication Union.* <http://handle.itu.int/11.1002/pub/80f875fa-en> (2018, березень, 29).

Основною характерною рисою італійських органів, що опікуються кібербезпекою є їх розгалуженість. Італія створила свою Першу комп'ютерну групу реагування на надзвичайні ситуації в 2013 р. Ця група була створена згідно зі Стратегією кібербезпеки і є Підрозділом Міністерства економічного розвитку. З інших органів можна відмітити Відділ кібербезпеки, який має повноваження для реагування на інформаційну кризу і є у підпорядкуванні Кабінету Міністрів[1].

Серед органів Італії, які займаються висвітленням діяльності захисту кіберпростору можна відмітити Департамент інформаційної безпеки, який аналізує та оцінює останні тенденції і загрози, а також проводить освітню політику направлену на популяризацію досягнутих результатів в цій сфері. Італія до того ж створила орган, що називається Управління по захисту персональних даних. Він займається тим, що реагує та висвітлює неправомірні дії з персональними даними. В поліції є підрозділ, який займається боротьбою з кіберзлочинністю та захистом критично важливої інфраструктури та є відповідальним за проведення заходів, що спрямовані на профілактику кіберзлочинності і захисту інфраструктури[2].

Перелічені органи за результатами звіту 2017 р. мають дуже високі державні стандарти, але в категорії професійних стандартів в Італії все ще бракує спеціалістів. Як для Італії так і для Іспанії необхідним завданням на сучасному етапі є підвищення галузевих стандартів для професіоналів та залучення нових спеціалістів у сфері безпеки кіберпростору[3].

В Іспанії органи, які опікуються безпекою кіберпростору є: Рада національної безпеки, Урядова комісія, делегована до цієї Ради, Спеціальний комітет з кібербезпеки та Спеціальний ситуаційний комітет, який діє за допомогою Ситуаційного центру департаменту національної безпеки[4]. Також в Іспанії створений у 2007 р. і діє CNPIC – Національний центр захисту інфраструктури та кібербезпеки. Він є органом, що відповідає за популяризацію, координацію та нагляд за всіма політиками та діями, пов'язаними з захистом критичної інфраструктури Іспанії та кібербезпеки в рамках Міністерства внутрішніх справ.

Іспанія та Італія в двох категоріях: організаційних можливостей та створених можливостей показують різні результати. Так зі створених можливостей Іспанія є лідером, а Італія показує середній результат. Стратегія кібербезпеки та рівень стандартизації органів двох державах знаходяться на середньому рівні. Іспанія значно випереджає Італію за показниками в сфері індустрії програмного забезпечення, а також у попередженні громадськості щодо кіберзагроз, тому державне забезпечення іспанських громадян інформацією та підтримка державного забезпечення Іспанією впливають на лідерство країни в цих галузях[5].

Обидві держави демонструють дуже високий показник у створенні практичних методів та технік, що сприяють професійному розвитку та підготовки галузевих проектів у сфері кібербезпеки[6].

Стимуляційні механізми, які направлені на попередження загроз в Італії є досить прогресивними. У сфері технічного забезпечення можна відзначити унікальну ініціативу в Італії щодо створення платформи обміну інформацією у напрямку можливих неправомірних транзакцій, фінансового шахрайства та потенційних кібератак на банківські системи, що сформована між банками та органами правопорядку[7].

При підтримці UniCredit, національного агентства по боротьбі зі злочинністю Великої Британії та глобального центру кібербезпеки система була створена у 2013 р. Цей проект був дуже успішним і тому в 2015 р. цю ініціативу було продовжено і як результат цей проект стимулював створення

[1] Hathaway, M., Demchak, C., Kerben, J., McArdle, J., Spidalieri, F. Italy Cyber Readiness at a Glance. The Potomac Institute for Policy Studies. < www.potomacinstitute.org/images/CRI/PIPS_CRI_Italy.pdf> (2018, березень, 29).
[2] Hathaway, M., Demchak, C., Kerben, J., McArdle, J., Spidalieri, F. Italy Cyber Readiness at a Glance. The Potomac Institute for Policy Studies. < www.potomacinstitute.org/images/CRI/PIPS_CRI_Italy.pdf> (2018, березень, 29).
[3] Global Cybersecurity Index, year: 2017 (International Telecommunication Union). *The Official website of the International Telecommunication Union.* <http://handle.itu.int/11.1002/pub/80f875fa-en> (2018, березень, 29).
[4] Estrategia de ciberseguridad nacional (2013). *Sitio oficial del Departamento de Seguridad Nacional.* <http://www.cnpic.es/Biblioteca/Legislacion/Generico/20131205_ESTRATEGIA_DE_CIBERSEGURIDAD_NACIONAL.pdf> (2018, березень, 31).
[5] Global Cybersecurity Index, year: 2017 (International Telecommunication Union). *The Official website of the International Telecommunication Union.* <http://handle.itu.int/11.1002/pub/80f875fa-en> (2018, березень, 29).
[6] Global Cybersecurity Index, year: 2017 (International Telecommunication Union). *The Official website of the International Telecommunication Union.* <http://handle.itu.int/11.1002/pub/80f875fa-en> (2018, березень, 29).
[7] Hathaway, M., Demchak, C., Kerben, J., McArdle, J., Spidalieri, F. Italy Cyber Readiness at a Glance. *The Potomac Institute for Policy Studies.* <www.potomacinstitute.org/images/CRI/PIPS_CRI_Italy.pdf> (2018, березень, 29).

аналогічних ініціатив в країнах ЄС, що перейняли досвід Італії. Аналізуючи дані, ця система сприяє обміну інформацією та надає сповіщення про неправомірні дії щодо персональних даних[1].

Переходячи до сфери кооперації можна визначити, що кооперація Іспанії знаходиться на середньому рівні, в той час як Італія показує дуже високі результати в цій сфері[2].

Прикладом може слугувати співробітництво з Великою Британією, країнами ЄС та США. Ця співпраця допомогла створити нові документи, розвинути італійську сферу кібербезпеки та покращити національну стратегію кібербезпеки.

Але й Іспанія має успіхи у напрямку обміну інформацією між різними країнами і підрозділами. В іспанській поліції є підрозділи, які опікуються кібербезпекою та співпрацюють з подібними органами країн ЄС. Прикладом, 2012 р. Національна поліція Іспанії заарештувала в Барселоні особу, відповідальну за найбільший кібернапад DDOS, що руйнувала Інтернет. Операція була проведена Бригадою з технологічних досліджень (UDEF Central), що належить Генеральному комісаріату судової міліції у співпраці зі штаб-квартирою поліції штату Каталонія. Поліція Нідерландів, Німеччини, Сполученого Королівства та Сполучених Штатів також брала участь на міжнародному рівні (справу було відкрито в Нідерландах)[3].

Італію з Іспанією також поєднує проект створення центру кібербезпеки який матиме назву «Центр Євросередземноморської кібербезпеки». Ця ініціатива повинна залучити більше інвестицій до Італії а також дипломатично покращити роль Італії в міжнародних відносинах[4].

Ця та інші ініціативи щодо покращення кібербезпеки характеризують Італію, як країну яка є більш залучена до міжнародних процесів мережевої та інформаційної безпеки. Обидві країни майстерно просувають ініціативи, які направлені на розвиток зв'язків з різними країнами ЄС та НАТО і просувають свої проектні пропозиції через ООН, НАТО, Раду Європи та через інші механізми. В той же час, Міністерство іноземних справ Італії також координує різні проекти в сфері кібербезпеки і частина повноважень відомства стосуються питань кібербезпеки. Відділ кібербезпеки підзвітний кабінету міністрів є важливим елементом у проведенні дипломатичних переговорів та реагування на різні кризові явища в Італії та Європейському регіоні[5].

Згідно з італійською білою книгою 2015 р. щодо сфери міжнародної оборони та безпеки, Італія почала створення об'єднаного командування операцій в кіберпросторі, яке буде повністю сформоване до кінця 2019 р. Це командування було створено з метою військової протидії кіберзагрозам і як зазначається в документах доповіді, розробленої Потомакським інститутом політичних досліджень, кіберпростір є зараз п'ятою сферою ведення бойових дій, тому є дуже важливим для захисту. Модель такого командування була взята з аналогічної структури США і метою такого командування буде створення організаційної структури та технічних можливостей для повноцінної роботи, також це підбір персоналу, який буде відповідати за оперативне планування у військових операціях у сфері інформаційного забезпечення. Також до повноважень органу будуть відноситись реагування на кризові та критичні ситуації, проведення різних військових навчань, що будуть направлені на укріплення кібероборонного потенціалу[6].

Висновок. Таким чином, узагальнюючи кібербезпекові можливості Іспанії та Італії на сучасному етапі:

1) за загальною оцінкою, Італія та Іспанія мають дуже високі показники глобального індексу кібербезпеки, але Іспанія як держава-лідер в галузі кібербезпеки за певними оціночними показниками випереджає Італію.;

---

[1] Hathaway M., Demchak C., Kerben J., McArdle J., Spidalieri F. Italy Cyber Readiness at a Glance. *The Potomac Institute for Policy Studies.* <www.potomacinstitute.org/images/CRI/PIPS_CRI_Italy.pdf> (2018, березень, 29).

[2] Global Cybersecurity Index, year: 2017 (International Telecommunication Union). *The Official website of the International Telecommunication Union.* <http://handle.itu.int/11.1002/pub/80f875fa-en> (2018, березень, 29).

[3] Colapsó Internet. La Policía Nacional detiene en Barcelona al responsable del mayor ciberataque de denegación de servicio DDOS de la historia. *Dirección General de la Policía*. <https://www.policia.es/prensa/20130428_1.html> (2018, березень, 31).

[4] Hathaway, M., Demchak, C., Kerben, J., McArdle, J., Spidalieri, F. Italy Cyber Readiness at a Glance. *The Potomac Institute for Policy Studies.* <www.potomacinstitute.org/images/CRI/PIPS_CRI_Italy.pdf> (2018, березень, 29).

[5] Hathaway, M., Demchak, C., Kerben, J., McArdle, J., Spidalieri, F. Italy Cyber Readiness at a Glance. *The Potomac Institute for Policy Studies.* <www.potomacinstitute.org/images/CRI/PIPS_CRI_Italy.pdf> (2018, March, 29).

[6] Hathaway, M., Demchak, C., Kerben, J., McArdle, J., Spidalieri, F. Italy Cyber Readiness at a Glance. *The Potomac Institute for Policy Studies*. <www.potomacinstitute.org/images/CRI/PIPS_CRI_Italy.pdf> (2018, March, 29).

2) Іспанія у чотирьох категоріях права у сфері захисту кіберпростору: кримінальне право та кібербезпекове право, кібербезпекова підготовка, а також у загальному індексі правових заходів отримала найвищі оцінки. Італія лише в сфері кібербезпекового права має найвищі оцінки а решта правових заходів знаходиться на найнижчому рівні.

3) За технічними можливостями для організації кібербезпеки обидві країни мають дуже високі показники. Іспанія має середню оцінку, а Італія має найвищу оцінку. В двох країнах створені національні команди які займаються відповідним реагуванням на інциденти у кіберпросторі та відновленням функціонування ураженого інформаційного середовища.

4) Органи Італії та Іспанії, які реалізують кібербезпеку за результатами звіту 2017 р. мають дуже високі державні стандарти, але в категорії професійних стандартів в Італії все ще бракує спеціалістів. Як для Італії так і для Іспанії необхідним завданням на сучасному етапі є підвищення галузевих стандартів для професіоналів та залучення нових спеціалістів у сфері безпеки кіберпростору.

5) Щодо категорій організаційних можливостей та створених можливостей Італія та Іспанія мають різні показники. Так зі створених можливостей Іспанія є лідером, а Італія показує середній результат. Стратегії кібербезпеки та рівень стандартизації органів держав мають середній рівень. Однак, Іспанія значно випереджає Італію за показниками в сфері індустрії програмного забезпечення й у попередженні громадськості щодо кіберзагроз. Відтак, державне забезпечення іспанських громадян інформацією та підтримка державного забезпечення Іспанією впливають на лідерство країни в цих галузях.

6) Італію та Іспанією поєднує проект створення центру кібербезпеки який матиме назву «Центр Євросередземноморської кібербезпеки». Його метою є залучення більше інвестицій до Італії, що зможе підвищити роль Італії в міжнародних відносинах. Також обидві південні країни ЄС опікуються у своїй діяльності захисту кіберпростору Стратегією кіберзахисту ЄС від 2013 р., що свідчить не тільки зміст Національних стратегій кіберзахисту країн, але й рік прийняття – 2013.

Порівняльний аналіз стану кібербезпекових можливостей Італії та Іспанії свідчить, що в Іспанії вищий рівень захисту даної сфери. Однак, це не захистило саму Іспанію від втручання у перебіг та висвітлення подій в Каталонії восени 2017 р. зокрема.

References:

1. Global Cybersecurity Index, year: 2017 (International Telecommunication Union). *The Official website of the International Telecommunication Union* <http://handle.itu.int/11.1002/pub/80f875fa-en> (2018, March, 29). [in English].
2. Hathaway, M., Demchak, C., Kerben, J., McArdle, J., Spidalieri, F. *Italy Cyber Readiness at a Glance. The Potomac Institute for Policy Studies.* <www.potomacinstitute.org/images/CRI/PIPS_CRI_Italy.pdf> [in English]. (2018, March, 29).
3. Negri, G. Facebook to monitor Italian election as EU debates Russian fake news. *The European Security Journal.* <https://www.esjnews.com/facebook-italy-russia-fake-news> [in English]. (2018, March, 29).
4. Henley, J., Solon, O. 'Petya' ransomware attack strikes companies across Europe and US. *The Guardian.* <https://www.theguardian.com/world/2017/jun/27/petya-ransomware-attack-strikes-companies-across-europe> [in English]. (2018, March, 29).
5. La trama rusa empleó redes chavistas para agravar la crisis catalana [The Russian plot used chavista networks to aggravate the Catalan crisis]. *Página Oficial. El Pais.* <https://politica.elpais.com/politica/2017/11/10/actualidad/1510341089_316043.html>. (2018, March, 31). [in Spanish].
6. Estrategia de ciberseguridad nacional, 2013 [National cybersecurity strategy, 2013]. *Sitio oficial del Departamento de Seguridad Nacional.* <http://www.cnpic.es/Biblioteca/Legislacion/Generico/20131205_ESTRATEGIA_DE_CIBERSEGURIDAD_NACIONAL.pdf> (2018, March, 31) [in Spanish].
7. Estrategia de seguridad nacional, 2017 [National security strategy, 2017]. *Sitio oficial del Departamento de Seguridad Nacional.* <http://www.dsn.gob.es/sites/dsn/files/Estrategia_de_Seguridad_Nacional_ESN%20Final.pd> [in Spanish]. (2018, March, 31).
8. La seguridad de ciberespacio como garantía de la integridad de España, por María García López [The security of cyberspace as a guarantee of the integrity of Spain, by María García López]. *Página Oficial del Diariocritico. Sábado 9 de diciembre de 2017* <https://www.diariocritico.com/opinion/maria-garcia-lopez/seguridad-de-ciberespacio> (2018, March, 31) [in Spanish].
9. Colapsó Internet. La Policía Nacional detiene en Barcelona al responsable del mayor ciberataque de denegación de servicio DDOS de la historia [The Internet has collapsed. The National Police stops in Barcelona the person responsible for the biggest DDOS cyber-attack in history]. *Dirección General de la Policía* <https://www.policia.es/prensa/20130428_1.html> (2018, March, 31) [in Spanish].