DOI: [10.32702/2307-2105-2020.10.70](https://doi.org/10.32702/2307-2105-2020.10.70)

УДК 339.9

*Г. А. Іващенко,
к. е. н., доцент кафедри міжнародного бізнесу та економічного аналізу,
Харківський національний економічний університет імені Симона Кузнеця. Україна
ORCID ID: 0000-0001-6581-0862
Д. М. Карталія,
студентка 3 курсу, факультет консалтингу і міжнародного бізнесу,
Харківський національний економічний університет імені Симона Кузнеця. Україна
ORCID ID: 0000-0002-6431-6974*

АНАЛІЗ ВПЛИВУ ПОЛІТИЧНИХ ФАКТОРІВ СЕРБІЇ НА МІЖНАРОДНУ БЕЗПЕКУ

*G. Ivashchenko
PhD in Economics, Associate Professor of the Department of International Business and Economic
Analysis, Simon Kuznets Kharkiv National University of Economics, Ukraine
D. Kartaliya
3-rd year student, Faculty of Consulting and International Business,
Simon Kuznets Kharkiv National University of Economics, Ukraine*

ANALYSIS OF THE INFLUENCE OF SERBIA'S POLITICAL FACTORS ON INTERNATIONAL SECURITY

У статті досліджується актуальна проблема визначення рівня ступеню безпекової політики Сербії на міжнародній арені і його впливу на сучасний стан зовнішніх відносин у контексті вступу до ЄС. Оцінка рівня захисту даних Сербії допомагає висвітлити аспекти політики національної безпеки. Завдяки проведеному кластерному аналізу країн Європейського регіону було визначено позиції держав щодо рівню захищеності інформаційних даних. Також досліджується актуальна проблема вступу Сербії до ЄС, головні чинники, що впливають на процес інтеграції однієї з провідних країн Балкан до європейської спільноти, відношення громадян Сербії щодо членства в ЄС та атрибутивне питання щодо краю Косово і Метохія, вирішення якої є головним визначальним фактором вступу.

Проведено кластеризацію країн за рівнем міжнародної безпеки. Кластеризацію проведено на основі таких підгруп показників: безпеки країн, інформаційної захищеності країн та соціальної адаптованості країн. В якості показників безпеки країн запропоновано індекс криміналу та індекс безпеки. Показниками інформаційної захищеності країн визначено індекс інтернет-користувачів у % до населення, індекс розвитку інновацій, індекс розвитку людського потенціалу. Показники соціальної адаптованості країн сформовано як індекс свободи преси, індекс політичних прав, індекс демократії, індекс сприйняття корупції, індекс соціального розвитку.

Кластеризація країн характеризує, що під час даного дослідження Сербія не змінювала свої позиції з 2014 по 2018 роки, що свідчить про сталий розвиток держави на середньому рівні.

Натомість, Україна та Російська Федерація знаходяться на низькому рівні розвитку міжнародної економічної безпеки, що свідчить про відсутність кардинальних змін у державній політиці [13]. Згідно до проведеного кластерного аналізу можна зазначити, що Велика Британія, Франція та Іспанія мають найвищий рівень захисту власних національних інтересів та активно підвищують власні позиції за рахунок дотримання основних демократичних принципів.

Сучасні інтеграційні процеси Сербії все більше привертають увагу міжнародної спільноти. Інтеграцію Сербії до Європейського Союзу розуміють як необхідну складову для покращення рівня життя, процесів виробництва, інфраструктури в умовах повного реформування устрою держави. Тим не менш зовнішньополітичні пріоритети Сербії, закладені в інтеграційних процесах, у яких бере участь країна, крім численних переваг, несуть і численні виклики для інформаційної безпеки країни.

The article deals the actual problem of determining the level of security policy of Serbia in the international arena and its impact on the current state of foreign relations in the context of EU accession. Assessing the level of data protection in Serbia helps to highlight aspects of national security policy. The positions of the states on the level of protection of information data were determined with the cluster analysis of the countries of the European region. It also examines the current problem of Serbia's accession to the EU, the main factors affecting the integration process of Serbia into the European community, the attitude of Serbian citizens on EU membership and the attributive issue of Kosovo and Metohija which solution of this problem determines process of accession.

The countries have been clustered according to the level of international security. Clustering was carried out on the basis of the following subgroups of indicators: security of countries, information security of countries and social adaptability of countries. The crime index and the security index are proposed as indicators of security of the countries. Indicators of information security of countries are determined by the index of Internet users in% of the population, the index of innovation development, the index of human development. Indicators of social adaptability of countries are formed as an index of freedom of the press, an index of political rights, an index of democracy, an index of perception of corruption, an index of social development.

The clustering of countries characterizes that during this study, Serbia did not change its position from 2014 to 2018, which indicates the sustainable development of the state at the average level. Instead, Ukraine and the Russian Federation are at a low level of development of international economic security, which indicates the absence of radical changes in public policy [13]. According to the cluster analysis, it can be noted that the United Kingdom, France and Spain have the highest level of protection of their own national interests and actively improve their own positions by adhering to basic democratic principles.

Serbia's current integration processes are increasingly attracting the attention of the international community. Serbia's integration into the European Union is understood as a necessary component for improving living standards, production processes, infrastructure in the context of a complete reform of the state system. Nevertheless, Serbia's foreign policy priorities inherent in the country's integration processes, in addition to numerous benefits, also pose numerous challenges to the country's information security.

Ключові слова. *Інформаційний захист; безпека; Сербія; ЄС; Косово і Метохія; міжнародна економічна безпека.*

Keywords. *Information Security; Security; Serbia; EU; Kosovo and Metohija; International Economic Security.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. На сьогоднішній день майже у всіх мовах та культурах слово безпека

застосовується в найрізноманітніших соціальних сферах, таких як політика, охорона здоров'я, інформатика, екологія, спорт, психологія, економіка та фінанси, архітектура тощо. У політичному дискурсі безпека займає особливе, можливо, навіть центральне місце. Політичні особи, які хочуть підкреслити екзистенційну значимість наявної проблеми і, таким чином, поставити її на перше місце порядку денного, кажуть, що вона є важливою для глобальної, національної та регіональної безпеки. В науковій роботі доцільно поставити акцент на формування концепції, сприйняття викликів євроінтеграції для Сербії та факторів ризику, безпек та загроз для державного апарату Республіки Сербія та виявлення її місця за рівнем міжнародної безпеки серед інших країн.

Актуальність проблеми визначається потребою аналізу політики Сербії і визначення ступеню її безпеки на загальнонаціональному та міжнародному рівнях.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми і на які спирається автор, виділення не вирішених раніше частин загальної проблеми, котрим присвячується означена стаття. Серед сербських дослідників слід відзначити роботи та аналітичні дослідження Венцислава Буїча – директора Фонду євроатлантичного співробітництва Сербії, а також українських та зарубіжних аналітиків з безпекової, військової та політичної сфери. Значна увага приділяється аналізу питання інформаційної безпеки та євроінтеграційним процесам Сербії в українсько-сербських періодичних виданнях та новинах, редактором яких є Борис Варга – сербський та український журналіст, публіцист. Постійний співпрацівник декількох ЗМІ та організацій: балканський кореспондент радіо та web «Українська служба Бі-Бі-Сі», аналітик веб-порталу «Al Jazeera Balkans», а також Гельсінської спілки з прав людини.

Формулювання цілей статті (постановка завдання). Мета наукового дослідження полягає у визначенні рівня ступеню безпекової політики Сербії на міжнародній арені і його впливу на сучасний стан зовнішніх відносин у контексті вступу до ЄС. Також висвітлення проблеми допомагає краще зрозуміти проблему інформаційного захисту даних у Сербії та висвітлити деякі менш знайомі аспекти політики національної безпеки.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Міжнародна безпека – система міжнародних відносин, що заснована на дотриманні усіма державами загально визнаних принципів і норм міжнародного права, виключає вирішення спірних питань і розбіжностей між ними за допомогою сили або загрози [9]. На сучасному етапі розвитку суспільства на міжнародну безпеку чинять безпрецедентно важливий вплив інформаційні фактори.

Інтернет сприяє розвитку електронного бізнесу (e-business), електронного банкінгу (e-banking), інтернет-магазини (e-shopping), дистанційного навчання (e-learning), маркетингу через електронні засоби масової інформації, що додатково вплинуло на зростання обміну даними між представниками різних культур в глобальному середовищі. У той же час усі переваги розвитку ІКТ є джерелом потенційних атак на конфіденційну інформацію, які можуть стати доступними для сторонніх осіб, або бути зміненими та знищеними [4]. Тому своєчасне інформування, підвищення обізнаності, корекція звичок стосовно користування Інтернет-ресурсами та надання відповідної інформації про ризики безпеки та шляхи усунення наслідків інцидентів мають першорядне значення. Швидкий, надійний та ефективний обмін інформацією може призвести до того, що органи державної влади, підприємства та громадяни не вживають своєчасних та адекватних заходів щодо захисту своїх систем та пристроїв. Такі масштабні інциденти можуть поставити під загрозу функціонування держави, економіки та суспільства, саме тому визначення ІКТ-систем, які мають особливе значення, щодо яких існує юридичний обов'язок піклуватися про безпеку інформації відповідно до чинного законодавства [6].

Таким чином, відповідно до наявної Стратегії розвитку 2017-2020 – створено Національний центр управління ризиками безпеки в системах ІКТ (Національний CERT) в рамках Регулюючого агентства з питань електронних комунікацій та поштових послуг (RATEL), завданням якого є збір та обмін інформацією про ризики безпеки для суспільства і влади Сербії [5]. Національний CERT повинен співпрацювати з подібними організаціями інших країн, враховуючи глобальний характер проблем інформаційної безпеки. Завдання національного CERT полягає у співпраці з відповідними міжнародними установами у галузі інформаційної безпеки, такими як ОБСЄ [7].

Для досягнення поставленої вище мети, по-перше, слід розглянути правову складову системи захисту інформації як головний чинник функціонування національної та економічної безпеки. Швидкий розвиток технологій також призвів до появи складних організаційних систем. Внаслідок цього уряд Сербії запровадив розвитку інформаційної безпеки за період з 2017 по 2020 роки.

Закон про інформаційну безпеку («Офіційний вісник РС», № 6/16 - далі: Закон) створив основу для створення та впровадження всеосяжної бази захисту даних в галузі інформаційної безпеки [1]. Закон регламентує заходи щодо захисту від ризиків безпеки в системах ІКТ, що мають особливе значення, обов'язки операторів системи ІКТ, що мають особливе значення в управлінні та використанні систем ІКТ та визначає компетентні органи щодо здійснення заходів безпеки, координації між факторами безпеки та контролю за належним виконанням передбачених заходів.

Опитування ЮНІСЕФ, яке було проведене в 2014 році на території Республіки Сербія, встановило, що понад 90% учнів старших класів та середніх шкіл мають мобільні телефони, і близько 90% дітей користуються Інтернетом [2]. Це ж дослідження виявило високі показники кіберзлочинності в Інтернеті та впливу цифрового насильства.

На рис. 1. наведено світовий рейтинг захисту інформації Сербії, що має 48 178 кількість захищених Інтернет-серверів за 2018 рік. Захищений сервер – це сервер, що використовує технологію шифрування при операціях в Інтернеті [27].

Рис. 1. Кількість захищених інтернет-серверів Сербії за 2018 рік

Згідно до поданого опитування половина опитаних викладачів сказали, що вони не мають належних навичок роботи з комп'ютером та Інтернетом і не знають як захистити конфіденційну інформацію та недостатньо проінформовані про цифрове насильство. Тож, опитування ЮНІСЕФ за 2016 рік, «Дослідження рівня обізнаності про потенційні Інтернет-ризики серед дітей у віці 8-17 років», трохи більше 50 відсотків батьків вважають не повністю здатними забезпечити допомогу та підтримку дитині, яка страждає від кібербулінгу [15].

Рис 2. Світовий рейтинг Інтернет-користувачів у % до населення Сербії

На рис. 2. наведено світовий рейтинг Інтернет-користувачів у % до населення Сербії, що складає 70,3 (%) за 2017 рік. Наявна стратегія визначає діяльність влади, яка має розвивати інформаційне суспільство в Сербії, що повинно відповідати новим викликам розвитку ІКТ (нові аспекти безпеки, загроза конфіденційності, технологічна залежність, недостатня сумісність інституцій, відкриті питання щодо захисту інтелектуальної власності, тощо). Стратегія встановлює, що до 2020 року всі ці аспекти будуть врегульовані в Сербії. Розрахункова кількість інтернет-користувачів як відсоток від усього населення. Цей показник вказує на користування Інтернетом з усіх можливих гаджетів (у тому числі мобільних телефонів) протягом останніх 12 місяців [26].

Таким чином, загальна мета Стратегії – розвивати та вдосконалювати інформаційну політику та безпеку в Республіці Сербія, підтримувати її на належному рівні, оскільки прийняття нормативно-правових актів у цій галузі визначає ІКТ-система, що має особливе значення та впливає заходи щодо національної безпеки [3].

Щодо подальшого дослідження інформаційно-аналітичного забезпечення економічної безпеки Республіки Сербія було виконано кластерний аналіз. Кластерний аналіз (англ. data clustering) – завдання розбиття об'єктів (ситуацій) на підмножини, що називаються кластерами, так, щоб кожен кластер складався зі

схожих об'єктів, а об'єкти різних кластерів істотно відрізнялися. Кластерний аналіз застосовується в різних сферах і галузях. Він працює навіть тоді, коли даних мало і не виконуються вимоги нормальності розподілу випадкових величин й інші вимоги класичних методів статистичного аналізу.

На базі кластерного дослідження і статистичних показників ми провели аналіз певних країн Європейського регіону, що дало можливість визначити приналежність кожної країни до підгруп з різним рівнем інформаційної захищеності.

Для проведення кластерного аналізу основних показників Сербії були відібрані країни з високим (Франція, Велика Британія, Іспанія), середнім (Угорщина, Греція, Румунія) та низьким (Україна, Російська Федерація) розвитком за такими критеріями як: територіальне сусідство (Угорщина, Румунія, торгові партнери (Російська Федерація Франція), країни що планують вступити до ЄС (Україна), країни, що планують вийти з ЄС (Велика Британія), країни, що зазнали кризового стану будучи членом ЄС (Греція) та країни, що мають проблеми зі збереженням територіальної цілісності (Іспанія). Наявні показники були вибрані за методом приналежності до інформаційної захищеності, соціального забезпечення та безпеки кожної з приведених держав. Враховуючи важливість і широту сфери інформаційної безпеки, уряд приймає цю стратегію з метою розвитку та вдосконалення інформаційної безпеки в Республіці Сербія [4]. Відтак нормативно-правова база інформаційної безпеки 2017-2020 роки складається з відповідних законів сфери захисту інформації, що регулюється (табл. 1).

Основні показники за якими було проведено дослідження розвитку стану захищеності кожної з наявних країн за даними Світового атласу даних Кноета.

Таблиця 1.
Показники міжнародної економічної безпеки країн

Показники	Підгрупи
Індекс криміналу, індекс безпеки	Показники безпеки країн
Індекс інтернет-користувачів у % до населення, індекс розвитку інновацій, індекс розвитку людського потенціалу	Показники інформаційної захищеності країн
Індекс свободи преси, індекс політичних прав, індекс демократії, індекс сприйняття корупції, індекс соціального розвитку	Показники соціальної адаптованості країн

Надані показники демонструють до якої з підгруп відносяться індекси за якими було проведено дослідження щодо рівня розвитку інформаційно-комунікаційного простору країн, що порівнювалися з показниками Республіки Сербії. Показники згруповані за принципом приналежності до кожної сфери діяльності держави, а саме: інформаційна, соціальна та безпекова.

Результати проведення кластерного аналізу країн 2018-2014 рр. надано на діаграмах (рис. 3. – рис. 4).

Рис. 3. Дендрограма стану міжнародної економічної безпеки країн за 2018 р.

Таблиця 2.
Інтерпретація результатів кластеризації країн за 2018 рік

Номер та назва кластеру	Назва країни
Перший кластер з середнім рівнем міжнародної економічної безпеки	Сербія, Румунія, Угорщина, Греція
Другий кластер з низьким рівнем міжнародної економічної безпеки	Україна, Російська Федерація
Третій кластер з високим рівнем міжнародної економічної безпеки	Велика Британія, Франція, Іспанія

Рис. 4. Індекс свободи преси країн в 2017 році

За індексом свободи преси, чим нижче показник, тим краща ситуація. Складна ситуація за індексом свободи преси в Російській Федерації. В Україні також не найкращий рівень індексу свободи преси.

Рис. 5. Дендрограма стану міжнародної економічної безпеки країн за 2017 р.

Рис. 6. Індекс інтернет-користувачів у % до населення країн за 2017 рік

В Україні найнижчий рівень інтернет-користувачів у % до населення. Найвищий рівень інтернет-користувачів у % до населення виявлено в Швеції.

В основному високий рівень міжнародної безпеки виявлено в таких країнах, як: Великобританія, Франція, Швеція та Іспанія.

Рис. 7. Дендрограма стану міжнародної економічної безпеки країн за 2016 р.

Дендрограма стану міжнародної економічної безпеки країн за 2015 р. представлена на рис. 8.

Рис. 8. Дендрограма стану міжнародної економічної безпеки країн за 2015 р.

На протязі всіх років Україна та Російська Федерація потрапляли до другого кластеру з низьким рівнем міжнародної безпеки. Рівень криміналу в Україна та Російська Федерація.

Рис. 9. Дендрограма стану міжнародної економічної безпеки країн за 2015 р.

Рис. 10. Рівень криміналу країн в 2017 році

Кластеризація країн за наявний 2018 рік характеризує, що під час даного дослідження Сербія не змінювала свої позиції з 2014 по 2018 роки, що свідчить про сталий розвиток держави на середньому рівні. Натомість, Україна та Російська Федерація знаходяться на низькому рівні розвитку міжнародної економічної безпеки, що свідчить про відсутність кардинальних змін у державній політиці [13]. Згідно до проведеного

кластерного аналізу можна зазначити, що Велика Британія, Франція та Іспанія мають найвищий рівень захисту власних національних інтересів та активно підвищують власні позиції за рахунок дотримання основних демократичних принципів.

Сучасні інтеграційні процеси Сербії все більше привертають увагу міжнародної спільноти. Інтеграцію Сербії до Європейського Союзу розуміють як необхідну складову для покращення рівня життя, процесів виробництва, інфраструктури в умовах повного реформування устрою держави. Тим не менш зовнішньополітичні пріоритети Сербії, закладені в інтеграційних процесах, у яких бере участь країна, крім численних переваг, несуть і численні виклики для інформаційної безпеки країни. 29 квітня 2008 року Республіка Сербія підписала Угоду про стабілізацію та асоціацію (SAA) з Європейським Союзом, яка набула чинності 1 вересня 2008 року. Цією угодою було закладено початок стадії відносин між Сербією та ЄС, підтверджено загальну перспективу членства Сербії в Європейському Союзі. Головна заява Сербії на членство в ЄС пролунала 22 грудня 2009 року, а статус кандидата до членів ЄС був наданий Європейською Радою лише 1 березня 2012 року [20].

Слід звернути увагу на те, що вже з 2008 року Європейський Союз зіткнувся з численними викликами. Фінансова, економічна та міграційна кризи, проблеми Греції, Брекзін, відсутність безпеки в рамках Союзу вплинули на виникнення розбіжностей всередині ЄС. Наявні кризові обставини сприяли поширенню популістських, переважно антиєвропейських рухів і партій по всій Європі [2]. Голова Європейської комісії Ж. К. Юнкер мав розпочати всебічну дискусію про майбутнє Європейського Союзу, зокрема про те, як зробити Союз більш ефективним, а процес прийняття рішень більш зрозумілим для громадян.

Необхідність реформування процесу прийняття рішень обумовлена суспільними вимогами до більш прозорого та ефективного управління, відновлення авторитету і демократичної легітимності Європейського Союзу. У ході реформування необхідно покращити процес прийняття рішень у сферах, що становлять спільний інтерес, таких як нелегальна міграція, функціонування ринку, спільна зовнішня політика і політика безпеки.

У березні 2017 року після референдуму щодо виходу Великобританії з Європейського Союзу (2016) Європейська Комісія презентувала Білу книгу про майбутнє Європи та шляхи її подальшого розвитку. У ній викладені можливі сценарії кооперації ЄС та його членів після врегулювання питання щодо Брекзиту у 2019 році [1]. Уже в травні 2018 року Центр європейської політики організував зустріч у Белграді, де були представлені результати цього широкого консультативного процесу. Слід підкреслити, що Белград є єдиним містом за межами Європейського Союзу у якому проводилися подібні дебати про майбутнє Союзу. Одним з висновків цієї зустрічі була промова колишнього голови сербської місії в Європейському Союзі Д. Лопандича, у якій він зазначив: «Необхідно відновити довіру до ЄС серед громадян нашої країни, а також довіру до Європи, довіру до її інститутів і здатності вирішувати проблеми» [9].

Тож, поки Велика Британія прагне виходу з ЄС, громадяни Сербії готуються до інтеграції в європейську спільноту. За даними останнього опитування, яке було проведено Міністерством європейської інтеграції (м. Белград) у грудні 2018 року, 55% громадян Сербії бажають, щоб Сербія стала частиною ЄС [2].

Згідно поданої діаграми – Міністерство європейської інтеграції Республіки Сербія провело опитування серед населення щодо набуття країною членства в ЄС. Тож, 55 % населення проголосували «ЗА», 25 % – «ПРОТИ», 10% – «НЕ ГОЛОСУВАЛИ Б ВЗАГАЛІ», інші 10% – «НЕ ЗНАЮТЬ/ НЕ НАДАЛИ ВІДПОВІДІ».

Рис. 11. Опитування населення Сербії щодо вступу країни до ЄС

На даний момент можна стверджувати, що Уряд Республіки Сербія визначив членство в ЄС як перший стратегічний пріоритет зовнішньої політики до 2025 року [11]. Створення умов для вступу до Європейського Союзу наразі розглядається як виняткова можливість для здійснення необхідних реформ у різних сферах

суспільства: від судової, фінансової, політичної системи до освіти, у якій переважним чином не було виявлено проблем Європейською Комісією. Більшість політичних діячів Західних Балкан вбачають процес сербської інтеграції до європейської спільноти необхідним, адже це нормалізує загальний рівень життя населення та заохотить провідні країни-донори ЄС до більш щільних інвестицій у розвиток економіки Сербії.

Надзвичайно важливо, щоб Сербія не втратила власних позицій у зовнішній політиці, а, навпаки, постала медіацією і досягла альтернативного вирішення спорів між головними стратегічними партнерами – ЄС та РФ [12]. Збоку інформаційної залежності від двох наведених кластерів регіону, опозиційні політичні сили Сербії наголошують на тому, що співпраця і членство в ЄС спровокує виникнення нових проблем з одним із провідних партнерів – Росією [15, с. 8]. На їхню думку, вступ країн до складу ЄС – дуже приваблива перспектива, але не для Сербії. Головним аргументом опозиції є приклад Великої Британії та Греції, які не задовольнили власні державні потреби і не забезпечили стабільності інформаційного захисту за допомогою членства у Союзі. Натомість опозиційні політичні блоки спровокували Сербію до активного діалогу і створення зони вільної торгівлі в рамках ЄЕС (Євразійський економічний союз), що є прототипом потужного наднаціонального об'єднання. Зовнішня політика провідної Балканської держави наразі є багатовекторною, тому цілком можливо, що зміни, які спрямовані на розширення багатьох функціонуючих сфер Сербії сприятимуть підвищенню регіональної ефективності країни і посилять захист ІКТ [17, с. 186]. У зв'язку з цим Сербії доведеться докласти додаткових зусиль, щоб підготуватися до нових зобов'язань, адже у жовтні 2019 вона набула повноцінного і рівноправного членства у ЄЕС. Одним із головних політичних викликів для Сербії, наразі, є захист інформації як складової національної безпеки, що є визначальним аспектом для рівної участі в політичному житті Європейського Союзу [14, с. 312]. Це ще одна причина, чому процес внутрішньої трансформації економічної, інформаційної, оборонної, правової та соціальної сфер повинен прискоритися.

Натомість, необхідно зазначити дві ключові позиції, до яких Сербія не має намірів звертатися. Це питання щодо історичної складової держави Косово і Метохія та членство країни в НАТО. Сучасна конфліктна ситуація між Косово та Республікою Сербія дуже непокоїть міжнародне співтовариство. Сербія, за Конституцією якої Косово і Метохія є автономним краєм у її складі, не визнає одностороннього проголошення державної незалежності Республіки Косово під керівництвом тимчасового самоврядування албанського населення [16, с. 54]. За своєю суттю тлумачення принципів міжнародного права щодо Косово є проявом «подвійних» стандартів. Спосіб вирішення косовської проблеми матиме безпосередній вплив на внутрішні процеси та зовнішню політику (в частині формування ставлення до схожих ситуацій в зонах розповсюдження національних інтересів) багатьох держав – Російської Федерації, США, Китаю, Іспанії, Туреччини, Македонії, безумовно, Сербії, та інших [14].

Міжурядові переговори про вступ Сербії до ЄС однозначно вказують на те, що існує певний тиск з боку міжнародної спільноти щодо питання інтеграції Сербії не тільки до ЄС, але й до воєнно-політичного альянсу – НАТО [13]. Цей факт слід сприймати як реальність, яка не зміниться під час переговорів ЄС з Сербією. Немоżliво не звернутися до ретроспективного аналізу подій 1999 року, коли міжнародне співтовариство втрутилося у збройний конфлікт між Сербією та Косово, у разі чого було знищено сотні тисяч мешканців на обох територіях. З березня по червень 1999 року НАТО провело проти Югославії військову операцію «Союзна сила», яка стала завершальним етапом Косовської війни і завдала суттєвої економічної та соціальної шкоди Сербії [12]. Безумовно, бомбардування мирного населення Сербії посилює негативне ставлення країни до участі у військово-політичному блоці і союзу держав, що підтримували «мирну» акцію щодо Косово.

Таким чином, подальша перспектива Сербії на здобуття членства в ЄС не в останню чергу залежить від політичних настроїв у Сербії та провідних країнах регіону. На користь переваг членства з ЄС можна зазначити, що Європа поступово змінює самодостатність відносно США, підкреслює власні інтереси і цінності. Приєднавшись до ЄС, Сербія може отримати значні додаткові ресурси для подолання поточних, як внутрішніх, так і зовнішніх, проблем у галузі інформаційного захисту.

Інформаційно-комунікаційні технології не тільки вчинили вплив на зміни у політиці та владі, але й створили нові симбіотичні суб'єкти, що провокують зміни у площині взаємозалежності міжнародних акторів щодо співпраці на політичній арені. Тож, ІКТ все більше трансформується у взаємодію людей, бізнесу та державних установ. Загальні зміни у всіх аспектах суспільства, що забезпечуються застосуванням ІКТ, сприяють розвитку інформаційного суспільства.

У межах Європейського Союзу ІКТ визнані головним рушієм економічного зростання та інновацій, а серед семи провідних ініціатив економічної стратегії «Європа 2020» – Цифрова програма для Європи, яка свідчить про важливість ІКТ у розвитку сучасних економік країн-членів. Разом із стратегією ЄС у галузі телекомунікацій і захисту інформації формує свій оборонно-інформаційний потенціал Республіка Сербія [8]. Безумовно, що вищезазначені фактори стверджують, що розвиток інформаційного суспільства має бути спрямований на використання потенціалу ІКТ для підвищення ефективності праці, економічного зростання, підвищення зайнятості та підвищення якості життя всіх громадян однієї з найрозвинутіших країн Балканського півострова. Тож, влада Сербії визначила, що двигуном розвитку інформаційного суспільства є:

відкритий, доступний та якісний доступ до Інтернету;

розроблена електронна комерція, включаючи: електронний уряд, електронна комерція, електронна справедливість, електронне здоров'я та електронна освіта. За розвитком інформаційного суспільства слід контролювати:

залучення всіх громадян Республіки Сербія, зокрема залучення соціальних груп з особливими потребами до регіонального розвитку та посилення місцевих ініціатив;

розвиток знань та навичок, пов'язаних з ІКТ, та посилення ролі ІКТ у системі освіти;

постійні інвестиції в наукові дослідження та інновації з метою виявлення, перегляду та максимального використання потенціалу ІКТ;

реагування на виклики, що постають перед ІКТ, такі як: нові аспекти безпеки, які порушують конфіденційність, технологічну залежність, відсутність сумісності та відкриті питання інтелектуальної власності;

координація та співпраця між державним, приватним та цивільним секторами [9].

На даному рис. 12. наведено світовий індекс мережевої готовності Сербії у 2016 році, який становить 4 бали з 7 можливих, що свідчить про гарний результат [13].

Рис. 12. Світовий індекс мережевої готовності Сербії у 2016 році

Підсумовуючи наявні інформаційні аспекти щодо державної політики захисту інформації, слід наголосити, що Стратегія розвитку інформаційного суспільства в Республіці Сербія 2017-2020 р.р – це акт уряду, який всебічно визначає основні цілі, принципи та пріоритети розвитку інформаційного суспільства та визначає діяльність, яку слід здійснити у період, що охоплюється цією стратегією.

Для Сербії як для країни-учасниці багатьох міжнародних організацій, позиція щодо вступу до ЄС є більш пріоритетною, ніж членство у НАТО. Саме інформаційна безпека – один із аспектів співпраці Сербії та НАТО, який останнім часом приділяє багато уваги. Не дивно, що в інтерв'ю з Європейськими Західними Балканами заступник генерального секретаря НАТО Роуз Гетемелер зазначила, що деякі з потенційних напрямів співпраці – це кібербезпека та кіберзахист. Адже постійне просування інформаційних технологій призвело до зміни характеру та форми загроз і спонукало НАТО до адаптації до нових обставин [15]. Таким чином, кіберзахист став частиною основної місії колективної оборони НАТО щодо усіх країн-членів. Альянс також працює над зміцненням навичок кібернавчання, навчання та навичок.

У відповідь на ці загрози та виклики на саміті у Уельсі у вересні 2014 року було затверджено план дій. Держави-члени визнали, що «міцні партнерські стосунки відіграють ключову роль у протидії кіберзагрозам та ризикам», і тому «продовжуватимуть активно займатися питаннями інформаційної безпеки з відповідними країнами-партнерами та з іншими міжнародними організаціями, у кожному конкретному випадку», – наявні факти продемонстровані у декларації саміту Уельсу. Вже у липні 2016 року члени НАТО «визнали кіберпростір як область операцій, в яких НАТО повинна захищати себе так само ефективно, як це відбувається в повітрі, на суші та в морі та зробити захист своїх інформаційних систем пріоритетним завданням, – йдеться на офіційному веб-сайті НАТО [10]. Співпраця з третіми країнами з питань кібербезпеки триває вже деякий час, і рамки такої співпраці можна знайти у різноманітних інструментах – від двосторонніх угод про співробітництво та індивідуальних програм до встановлених колективних програм співпраці.

У сфері кібербезпеки правова база Сербії базується на Законі про інформаційну безпеку, прийнятому нещодавно, у 2016 році. Закон, серед іншого, закликає створити орган координації щодо регулювань інформаційної безпеки, у тому числі, представників інших державних органів, академічної громади та громадянського суспільства. Крім того, у травні 2017 року була прийнята вже відома Стратегія розвитку інформаційного суспільства в Республіці Сербія до 2020 року як одна з шести пріоритетних напрямків, що передбачає безпеку систем ІКТ, інформаційну безпеку громадян, боротьбу з високотехнологічною злочинністю, інформаційну безпеку Республіки Сербія та міжнародне співробітництво [11]. Отже, прийнявши Стратегію, Сербія виконала своє зобов'язання у галузі інформаційної безпеки в процесі вступу до ЄС.

Звіт про дослідження інформаційної безпеки на Західних Балканах містить інформацію про те, що існують правові механізми боротьби з кіберзлочинністю. Однак, як стверджують автори, існує недостатня багато дисциплінарна освіта з питань кібербезпеки на рівні політики. Головним з факторів того, що були також

спроби підвищити рівень обізнаності населення з питань безпеки в Інтернеті загалом.

Щоправда, співпраця Сербії та НАТО в галузі кібербезпеки передбачена Індивідуальним планом дій партнерства (ІРАР), підписаним у 2015 році, який забезпечив основу для подальшого вдосконалення співробітництва без будь-яких наголошень щодо членства Сербії у НАТО. Таким чином, дотримуючись заявленого військового нейтралітету Сербії та спираючись на ІРАР, «Республіка Сербія хоче розширити свої можливості захисту критичних комунікаційних та інформаційних систем від кібератак за допомогою країн-членів НАТО» [12]. ІРАР передбачав, наприклад, розробку національної політики та стратегії в галузі кіберзахисту, прийняття необхідних законів та правил, механізмів державного рівня та міжнародних механізмів координації для ефективного реагування на кібератаки, тощо. Наразі Сербія досягла прогресу у виконанні рекомендованих норм, прийняття нових законів захисту і відповідної Стратегії, а отже зробила важливий крок на шляху євроінтеграції.

Хоча співпраця Сербії та НАТО в галузі кібербезпеки має невеликий процент розвитку, то з кожним роком вона має намір збільшуватися. Неможливо не згадати про те, що вже у 2007 році Сербія приєдналася до Програми миру та безпеки НАТО (SPS), і з часом процес інформаційної комунікації активізувався. Одним із ключових пріоритетів програми SPS є кіберзахист, який включає захист критичної інфраструктури, який передбачає обмін найкращими практиками, нарощування оборонного потенціалу та політики захисту національної безпеки та підтримку розвитку можливостей кіберзахисту. У 2017 році було проведено навчання за програмою SPS, під час якої державні службовці Управління Ради національної безпеки Сербії пройшли навчання з питань захисту інформаційних систем (INFOSEC) у ситуаціях реального життя. Політика INFOSEC вважається дуже важливою, оскільки може надати додатковий інструмент протидії кіберзагрозам. Тренінг проходив у Белграді та Таллінні з 30 жовтня по 10 листопада 2017 року. «Це була чудова можливість для нас посилити співпрацю між НАТО та Сербією в галузі інформаційної безпеки. Ми хотіли б підкреслити високу мотивацію та добрий дух групи, яка зробила цю подію успішною», - заявив генерал-майор Велло Лоема з Європейської ініціативи з кібербезпеки в Естонії, установи, яка організовувала навчання у сфері координації з Управлінням національної безпеки та Секретаріатом Сербії.

Отже, сфера інформаційної безпеки, безумовно, буде пріоритетною у довгостроковій перспективі для Республіки Сербії, адже захист національних інтересів і посилення комунікаційного зв'язку з країнами-членами НАТО створює можливості для вступу до ЄС. Натомість, Сербія є авангардом на території Балкан, а отже може стати месією і прикладом для південних країн, і навчити як саме потрібно запроваджувати політику захисту інформаційних технологій і відстоювати національні інтереси, незважаючи на співпрацю з колишніми агресорами, таким як НАТО.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Широкий взаємозв'язок соціальних, організаційних, технічних, фінансових, економічних та інших типів систем через національні кордони, заснований на застосуванні ІКТ та систем, створює складне міжнародне середовище, в якому відбувається динамічна взаємодія між різними суб'єктами Сербії. Соціальне та економічне процвітання, національна безпека та оборона Республіки Сербія безпосередньо та опосередковано залежать від ефективності мереж ІКТ, які поширюються всередині країни та за її межами в складних, динамічних і часто непередбачуваних умовах. Взаємодія на основі ІКТ є двосторонньою і має прямий вплив на національну безпеку.

Встановлення та розвиток інформаційної безпеки на національному рівні може бути досягнуто лише шляхом здійснення комплексних заходів, які одночасно здійснюються та координуються на державному та міжнародному рівнях. Для Сербії контакт з міжнародними партнерами є багатозаровим, активним та оптимальним процесом, оскільки він охоплює широке коло державних, неурядових та наднаціональних організацій на політичному, технічному та професійному рівнях. Основними міжнародними партнерами Республіки Сербія в цьому плані є Організація Об'єднаних Націй (ООН), Організація з безпеки і співробітництва в Європі (ОБСЄ), Європейський Союз (ЄС), Рада Європи (РЕ), політичні, економічні та оборонні організації та альянси, з якими Республіка Сербія уклала угоди про взаємне співробітництво.

Тож, для досягнення поставлених цілей міжнародного співробітництва Республіки Сербія необхідно налагоджувати та розвивати міжнародне співробітництво на двосторонній та багатосторонній основі з метою покращення національної та міжнародної інформаційної безпеки. Крім того, слід налагодити співпрацю для обміну інформацією, знаннями та досвідом з провідними міжнародними акторами щодо запобігання ризикам безпеки в ІКТ-системах. Безумовно, координаційна політика Республіки Сербії має бути спрямована на активну участь у міжнародних цивільних та військових навчаннях, які забезпечують розвиток інформаційного простору на всіх комунікаційних рівнях.

Таким чином, інформаційна безпека Республіки Сербія – це ключова частина всеохоплюючої національної безпеки, яка базується на інформаційній безпеці установ, сил, людей, систем, процесів, інформації та цінностей, що мають значення для безпеки та оборони країни.

Інформаційно-комунікаційна інфраструктура, послуги та дані оборонної системи мають особливе значення для політичного стану Республіки Сербія. Тому інформаційна безпека оборонної системи є однією з ключових складових подальшої стратегії розвитку та головним елементом на шляху до євроінтеграції Сербії.

Список літератури.

1. Strategija razvoja informacionog društva u Republici Srbiji do 2020. go- dine, 2010, Službeni Glasnik Republike Srbije [Електронний ресурс] // 5. – 2010. – Режим доступу до ресурсу: http://paragraf.rs/propisi/strategija_razvoja_informacionog_drustva_u_republici_srbiji.htm.
2. European Commission, Communication from the Commission Europe 2020, A Strategy for smart, sustainable and inclusive growth, COM (2010) 2020, Brussels, 3. 3. 2010 [Електронний ресурс] – Режим доступу до ресурсу: на http://eunec.vlor.be/detail_bestanden/doc014%20Europe%202020.pdf.
3. Zakon o organizaciji i nadležnosti državnih organa za borbu protiv viso- kotehnološkog kriminala, 2009., Službeni glasnik Republike Srbije br. 61/2005, 104/2009, [Електронний ресурс] – Режим доступу до ресурсу: <http://zakon.co.rs/zakon-o-organizaciji-i-nadleznosti-drzavnih-organa-za-borbu-protiv-visokotehnoloskog-kriminala.htm>.
4. Zakon o telekomunikacijama, 2006., Službeni glasnik Republike Srbije br. 44/2003 i 36/2006, [Електронний ресурс] – Режим доступу до ресурсу: www.mtid.gov.rs/wp_content/uploads/Dokumenti/Zakoni/Zakon_o_telekomunikacijama.pdf.
5. Kljajić, Z., Mandžuka, S., Škorput, P., 2010., Primjena ICT-a u upra- vljanju kritičnom infrastrukturuom u tranzicijskom zemljama, 18. Telekomunikacio- ni forum TELFOR 2010. Srbija, pp. 75–78.
6. Critical information infrastructure protection, 29. 06. 2011. [Електронний ресурс] – Режим доступу до ресурсу: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm.
7. CIIP Action Plan in its Communication on Critical Information Infrast- ructure Protection – ‘Protecting Europe from large scale cyber-attacked cyberdisruptions: enhancing, preparedness, (2009) 149, 2009. [Електронний ресурс] – Режим доступу до ресурсу: <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF>.
8. European Commission, Communication from the Commission Europe 2020, A Strategy for smart, sustainable and inclusive growth, COM (2010) 2020, Brussels, 3. 3. 2010. [Електронний ресурс] – Режим доступу до ресурсу: на http://eunec.vlor.be/detail_bestanden/doc014%20Europe%202020.pdf.
9. Zakon o Vojnobezbednosnoj agenciji i Vojnoobaveštajnoj agenciji, 2009., Službeni glasnik Republike Srbije br. 88/2009, [Електронний ресурс] – Режим доступу до ресурсу: http://paragraf.rs/propisi/zakon_o_vojnobezbednosnoj_agenciji_i_vojnoobavestajnoj_agenciji.html.
10. Informaciona bezbednost: Nova oblast saradnje Srbije i NATO? [Електронний ресурс] – Режим доступу до ресурсу: <https://europeanwesternbalkans.rs/informaciona-bezbednost-nova-oblast-saradnje-srbije-nato/>.
11. Informaciona bezbednost podataka gradjana na lokalnu [Електронний ресурс] – Режим доступу до ресурсу: <http://vrhvesti.rs/2018/12/informaciona-bezbednost-podataka-gradjana-na-lokalu/>.
12. STRATEGIJA RAZVOJA INFORMACIONOG DRUŠTVA U REPUBLICI SRBIJI DO 2020. GODINE [Електронний ресурс] – Режим доступу до ресурсу: https://www.paragraf.rs/propisi/strategija_razvoja_informacionog_drustva_u_republici_srbiji.html.
13. INFORMACIONA BEZBEDNOST PREDUSLOV DIGITALNOG RAZVOJA [Електронний ресурс] – Режим доступу до ресурсу: <https://www.pametnoibezbedno.gov.rs/vest/1489>.
14. Гальчинський А. Глобальні трансформації: концептуальні альтернативи. Методологічні аспекти / А. Гальчинський. Київ : Либідь, 2006. – 312 с.
15. Ковачевић. А. Економски односи Србије са ЕУ / А. Ковачевић. – Београд : Универзитет у Београду. Економски факултет, 2012. – 8 с.
16. Савчук К. Еволюція інституту міжнародно-правового визнання держав в сучасних умовах / К. Савчук // Юридичний журнал. – 2009. – №1. – С. 50 – 58.
17. Цховребов К. И. Проблемы статуса непризнанных и частично признанных государств в современном мире / К. И. Цховребов // Вестник Северо-Осетинского государственного университета им. К. Л. Хетагурова. – Владикавказ, 2013. – №4. – С.186 – 189.
18. Чумаченко О. А. Політика розширення Європейського Союзу в Західних Балканах: Основні ризики та шляхи їх подолання [Електронний ресурс] / О. А. Чумаченко. – Режим доступу : <http://vmv.kymu.edu.ua/v/p01/10%20chumachenko.pdf>.

References.

1. Službeni Glasnik Republike Srbije (2010), “Strategy for the development of the information society in the Republic of Serbia until 2020”, available at: http://paragraf.rs/propisi/strategija_razvoja_informacionog_drustva_u_republici_srbiji.htm (Accessed 10 Oct 2020).
2. European Commission (2020), “Communication from the Commission Europe 2020, A Strategy for smart, sustainable and inclusive growth”, available at: http://eunec.vlor.be/detail_bestanden/doc014%20Europe%202020.pdf (Accessed 10 Oct 2020).
3. Službeni glasnik Republike Srbije (2009), “Law on Organization and Competences of State Bodies for Combating High-Tech Crime”, available at: <http://zakon.co.rs/zakon-o-organizaciji-i-nadleznosti-drzavnih-organa-za-borbu-protiv-visokotehnoloskog-kriminala.htm> (Accessed 10 Oct 2020).
4. Službeni glasnik Republike Srbije (2006), “Law on Telecommunications”, available at: www.mtid.gov.rs/wp_content/uploads/Dokumenti/Zakoni/Zakon_o_telekomunikacijama.pdf (Accessed 10 Oct 2020).

5. Kljajić, Z. Mandžuka, S. and Škorput, P., (2010), "Application of ICT in critical infrastructure management in transition countries", 18. Telekomunikacioni forum TELFOR 2010 [18th TELFOR Telecommunication Forum 2010], Srbija, pp. 75–78.
6. European Commission (2011), "Critical information infrastructure protection", available at: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm (Accessed 10 Oct 2020).
7. European Commission (2009), "CIIP Action Plan in its Communication on Critical Information Infrastructure Protection – 'Protecting Europe from large scale cyber-attacked cyberdisruptions: enhancing, preparedness'", available at: <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF> (Accessed 10 Oct 2020).
8. European Commission (2020), "Communication from the Commission Europe 2020, A Strategy for smart, sustainable and inclusive growth", available at: http://eunec.vlor.be/detail_bestanden/doc014%20Europe%202020.pdf (Accessed 10 Oct 2020).
9. Službeni glasnik Republike Srbije (2009), "Law on the Military Security Agency and the Military Intelligence Agency", available at: http://paragraf.rs/propisi/zakon_o_vojnobezbednosnoj_agenciji_i_vojnoobavestajnoj_agenciji.html (Accessed 10 Oct 2020).
10. Anđelković, K. (2017), "Information security: A new area of cooperation between Serbia and NATO?", available at: <https://europeanwesternbalkans.rs/informaciona-bezbednost-nova-oblast-saradnje-srbije-nato/> (Accessed 10 Oct 2020).
11. VRH Vesti (2018), "Information security of local citizens' data", available at: <http://vrhvesti.rs/2018/12/informaciona-bezbednost-podataka-gradjana-na-lokalu/> (Accessed 10 Oct 2020).
12. Sl. glasnik RS (2010), "Information society development strategy in the Republic of Serbia until 2020", available at: https://www.paragraf.rs/propisi/strategija_razvoja_informacionog_drustva_u_republici_srbiji.html (Accessed 10 Oct 2020).
13. Pametno i bezbedno (2020), "Information security is a prerequisite for digital development", available at: <https://www.pametnoibezbedno.gov.rs/vest/1489> (Accessed 10 Oct 2020).
14. Hal'chyns'kyj A. (2006), Hlobal'ni transformatsii: kontseptual'ni al'ternatyvy. Metodolohichni aspekty [Global transformations: conceptual alternatives. Methodological aspects], Lybid', Kyiv, Ukraine.
15. Kovachevyh. A. (2012), Ekonomsky odnosa Srbyje sa EU [Serbia's economic relations with the EU], Univerzitet u Beogradu. Ekonomsky fakultet, Beograd.
16. Savchuk K. (2009), "The evolution of the institution of international legal recognition of states in modern conditions", Yurydychny zhurnal, vol.1, pp. 50 – 58.
17. Tskhovrebov K. Y. (2013), "Problems of the status of unrecognized and partially recognized states in the modern world", Vestnyk Severo-Osetynskogo gosudarstvennogo unyversyteta ym. K. L. Khetahurova. Vladykavkaz, vol.4, pp.186 – 189.
18. Chumachenko O. A. (2010), "EU Enlargement Policy in the Western Balkans: Key Risks and Ways to Overcome Them", available at: <http://vmv.kymu.edu.ua/v/p01/10%20chumachenko.pdf> (Accessed 10 Oct 2020).

Стаття надійшла до редакції 20.10.2020 р.