Bulletin of Taras Shevchenko National University of Kyiv.
Legal Studies, 2021; 2 (117): 30-38
УДК: 314
DOI: https:doi.org/10.17721/1728-2195/2021/2.117-6

ISSN 1728-2195
© Taras Shevchenko National University of Kyiv,
Publishing center "Kyiv University", 2021

С. Кавин, асп.
ORCID ID: 0000-0002-6189-3848

І. Брацук, канд. юрид. наук, доц.
ORCID ID: 0000-0003-0164-7407
Львівський національний університет імені Івана Франка, Львів, Україна

НОРМАТИВНО-ПРАВОВІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В НОВИХ ДЕРЖАВАХ-ЧЛЕНАХ ЄС

Статтю присвячено вивченню механізмів і специфіки особливостей нормативно-правового забезпечення інформаційної безпеки в нових державах-членах ЄС у контексті дослідження їхніх національних кіберстратегій як складової частини національної безпеки з метою їхньої інтеграції в єдину міжнародну багатовекторну систему захисту інформаційного простору.

У багатьох державах-членах Європейського Союзу, зокрема Болгарії, Румунії, Словаччині, Хорватії, Чехії, сформовано загальнодержавні мережі інформаційної безпеки, які здатні досить швидко акумулювати сили та засоби державних органів для протидії, зокрема і кіберзагрозам, тим самим забезпечуючи національну безпеку своїх країн. На основі проведеного дослідження встановлено, що у своїх стратегіях держави-члени ЄС, зокрема Центрально-Східного регіону: Болгарія, Румунія, Словаччина, Хорватія, Чехія, одностайні щодо своїх планів інтегрувати національні можливості кіберзахисту та розширити ресурси для протидії кібератакам. Кожна із цих країн також використовує міжнародне співробітництво для обміну інформацією про кібербезпеку та технічну допомогу. Разом із тим аналіз нормативно-правових та організаційних основ системи кібербезпеки держав-членів ЄС свідчить про домінантну роль спецслужб, зокрема і військових, у забезпеченні кібербезпеки держави, що пов'язано з характером кіберзагроз сьогодення, протидія яким потребує інструментарію (повноважень, форм і методів), притаманного виключно спеціальним – контррозвідувальним органам держави.

Ключові слова: держави-члени ЄС, інформаційна безпека, кібербезпека, інформаційний простір, норма права.

ВСТУП. Події останніх років чітко вказують на наявність кризи у сфері забезпечення інформаційної безпеки і на міжнародному, і на регіональному рівнях. Тому на перший план виходить вирішення питань саме належного законодавчого забезпечення інформаційної безпеки. У цьому контексті кожна держава Європейського Союзу як невід'ємну складову своєї стратегії національної безпеки прийняла національні стратегії кібербезпеки, задача яких – забезпечення ефективного механізму захисту інформаційного простору та протидії кібератакам на критично-важливі національні інфраструктури. У межах цього законодавчого акту майже в кожній державі Європейського Союзу з метою практичного забезпечення механізму захисту від кібератак критично-важливих національних інфраструктур, у межах відповідних інституцій, створено спеціальні органи швидкого реагування на кіберінциденти (CERT). А контроль і управління забезпеченням інформаційної безпеки, зокрема і кібербезпеки, покладено на державні силові інституції: оборонні відомства, відомства безпеки, відомства внутрішніх справ. У зв'язку із цим міжнародна співпраця, у т. ч. з Європейськими інституціями, стосовно уніфікованих підходів до боротьби з кіберзагрозами в інформаційному просторі, носить обмежений характер, оскільки інформація щодо національних критичних структур має статус секретної і відповідно охороняється національними законодавствами. Проте майже всі держави одностайні щодо своїх планів інтегрувати національні можливості кіберзахисту та розширити ресурси для протидії кібератакам у межах законодавчої бази Європейського Союзу.

Мета дослідження – вивчення особливостей нормативно-правового забезпечення інформаційної безпеки країн Центрально-Східної Європи в контексті дослідження їхніх національних кіберстратегій, як іманентної складової національної безпеки з погляду диверсифікації зовнішніх відносин у багатовекторній системі міжнародної безпеки.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ. Вивчаючи національне законодавство держав-членів ЄС у сфері забезпеченні інформаційної безпеки та протидії кіберзагрозам, а також досліджуючи їхню практику в цьому напрямку, ученими сформовано зауваження, суть яких полягає в тому, що поки не існує єдиної уніфікованої системи в цьому напрямку, кожна з держав має свої правові механізми щодо врегулювання вказаних питань і кожна з них має свою унікальну систему захисту інформації [23, с. 105–114], [24, с. 91–100], [27, с. 91–100].

Diego Acosta Arcarazo і Cian C. Murphy, зазначають, що набрання чинності Лісабонським договором надало ЄС нові повноваження у галузі права міжнародної безпеки, разом із тим Стокгольмська програма – це остання рамкова програма дій ЄС у сфері юстиції та внутрішніх справ, зокрема в питаннях співпраці між національними системами кримінального правосуддя. І поєднання нового Договору та Програми зробило безпеку та правосуддя ключовими сферами законодавчого розвитку в ЄС [29, с. 17] . На цьому робить акцент і Raphael Bossong, який зазначає, що важливий елемент співробітництва в галузі безпеки між країнами Європейського Союзу – це інтенсивний обмін інформацією між органами безпеки. Хоча у цій особливо чутливій області не слід очікувати якихось особливих кроків на шляху інтеграції. Однак наявні підходи до розвідувальної підтримки політики безпеки ЄС мають поглиблюватися та краще контролюватися [34, с. 6].

Професор д-р Удо Гельмбрехт зазначає, що забезпечення мережних та інформаційних систем Європейського Союзу у правовому полі має важливе значення для підтримки інтернет-економіки на основі впровадження нових ініціатив щодо подальшого покращення кіберстійкості та реагування на кіберзахист [38] . У цьому контексті Laszlo Kovacs у своїй роботі "Cyber Security Policy and Strategy in the European Union and NATO" [32, с. 16–24], а також Sevdalina Dimitrova, Stoyko Stoykov і Yosif Kochev у роботі "National Cybersecurity Strategies in Member States of the European Union" [37, с. 54–58] визначають стратегію кібербезпеки як базовий документ, створений в урядовому контексті, що відображає інтереси та правила

© Кавин С., Брацук І., 2021

безпеки роботи в кіберпросторі. Крім того, установлює основу для майбутнього законодавства, політики / стандартів, керівних принципів та інших рекомендацій щодо безпеки та кібербезпеки. Основні принципи кібербезпеки викладено у документах ЄС і НАТО.

Інформаційна безпека держав ЄС характеризується ступенем захищеності, а отже стійкістю основних сфер життєдіяльності (економіки, науки, техносфери тощо) щодо небезпечних (дестабілізаційних, деструктивних, таких, що суперечать інтересам країни, тощо) інформаційних впливів, причому як до впровадження, так і до вилучення інформації. Відповідно в багатьох Європейських документах присутнє визначення інформаційної безпеки, зокрема: в Європейських критеріях безпеки інформаційних технологій (Information Technology Security Evaluation Criteria (ITSEC)), які розроблені у країнах Європи (Франція, Німеччина, Нідерланди та Велика Британія) 1991 р., інформаційна безпека визначається так: *"Інформаційна безпека – це захист інформаційних ресурсів від несанкціонованого доступу з метою забезпечення конфіденційності; забезпечення цілісності інформаційних ресурсів шляхом їхнього захисту від несанкціонованої модифікації або знищення; забезпечення працездатності систем за допомогою протидії загрозам відмови в обслуговуванні"* [13].

Згідно з доповіддю Генеральної Асамблеї ООН A/55/40 (Report of the Human Rights Committee Volume II General Assembly Official Records Fifty-fifth Session Supplement No. 40 (A/55/40)) міжнародна інформаційна безпека визначається як *"стан міжнародних відносин, який виключає порушення світової стабільності та створення загрози безпеці держав і світової спільноти в інформаційному просторі"* [18].

У Повідомленні Європейської Комісії Європейському Парламенту, Раді Європи, Європейському Економічному Комітету і Комітету Регіонів "Мережна й інформаційна безпека: пропозиція щодо підходу до європейської політики" ("Network and Information Security:Proposal for a European Policy Approach") інформаційна безпека визначається так: *"Мережна й інформаційна безпека – це здатність мережі або інформаційної системи чинити опір випадковим подіям або зловмисним діям, які становлять загрозу доступності, аутентичності, цілісності та конфіденційності даних, що зберігаються або передаються, а також послуг, що надаються через ці мережі й системи"* [8].

В іншому Повідомленні Європейської Комісії Європейському Парламенту, Раді Європи, Європейському Економічному Комітету і Комітету Регіонів "Захист Європи від широкомасштабних кібератак і руйнувань: посилення рівня підготовленості, безпеки та стійкості" ("Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience") поняття інформаційної безпеки визначено так: *"Інформаційна безпека – захищеність від некоординованих національних підходів до безпеки інформаційних структур, безпекових інцидентів"* [9].

У ході розвитку нових ІТ-технологій головний акцент інформаційної безпеки міститься у площині кіберзахисту, що потребує якісно нової нормативно-правової платформи забезпечення інформаційної безпеки. Кібербезпека – це вже новий виток інформаційної безпеки, який спрямований саме на діджитал-середовище, в якому власне ми і перебуваємо. Нині кібербезпека – це не лише сам по собі захист інформації, а й захист усієї системи в інформаційному полі, в ІТ-полі (поле комп'ютерних технологій) у цілому і відповідає за три чинники: системи, процеси, люди.

У Лісабонському договорі (Treaty Of Lisbon Amending The Treaty On European Union And The Treaty Establishing The European Community (2007/C 306/01)) кібербезпека визначається так: *"Кібербезпека є однією зі складових інформаційної безпеки, що перебуває у повноваженні Верховного представника з питань спільної зовнішньої та безпекової політики"* [22].

Генеральний директор ENISA, професор д-р Удо Гельмбрехт у своєму виступі "Adequate and effective cybersecurity: state of play" на конференції з кібербезпеки, організованій австрійським головуванням у Раді Європейського Союзу, зазначив, що *"кібербезпека – захист інформаційного простору від кіберінцидентів і сторонніх провокаційних впливів"* [38].

У цьому ж контексті представляє інтерес досвід деяких країн Східної Європи, зокрема Болгарії, Румунії, Словаччини, Хорватії та Чехії.

Болгарія. У квітні 2016 р. Консультативна рада представила Парламенту Болгарії проєкт Національної стратегії кібербезпеки під назвою "Стійка до кібератак Болгарія 2020" (National Cyber Security Strategy Cyber Resilient Bulgaria 2020) [4] .

Цей проєкт окреслює кілька векторів становлення й розвитку сучасної й ефективної національної системи інформаційної безпеки, зокрема і кіберзахисту. Як зауважив Т. Ткачук, ці вектори спрямовано в бік інтеграції спільної Європейської системи інформаційної безпеки, зокрема це:

- генерування ініціатив, направлених на реалізацію законодавчих змін, пов'язаних з імплементацією Директиви Європейського Парламенту та Ради (ЄС) 2016/1148 від 6 липня 2016 р. про заходи для високого спільного рівня безпеки мережних та інформаційних систем на території Союзу;
- створення потужного широкоформатного потенціалу, у т. ч. наукового, для забезпечення кіберзахисту на основі тотального розширення мережі ІТ-інфраструктур;
- реалізація сучасної моделі обміну інформацією на основі використання хмарних технологій і нейронних мереж, відповідно забезпечення на цій основі ефективної координації дій між структурами, що відповідають за забезпечення кіберзахисту;
- розроблення та реалізація програм на законодавчому і на виконавчому рівнях щодо забезпечення фінансовими ресурсами та поповнення кадрового потенціалу кваліфікованими експертами з питань кібербезпеки, відповідних відомств, у компетенції яких входить забезпечення системи інформаційної безпеки, у т. ч. кібербезахисту, зокрема: Міністерство внутрішніх справ, Агентство національної безпеки, Міністерство оборони, Державне агентство розвідки;
- зміцнення співробітництва з Європейським Союзом та НАТО щодо забезпечення інформаційної безпеки, у т. ч. кіберзахисту [26, с. 62–67].

Щодо міжнародного співробітництва у сфері кіберзахисту, то плани Стратегії чітко зорієнтовано на створення і розширення діяльності Оперативного центру кіберзахисту. Ця задача реалізується відповідно до плану розвитку Збройних сил Болгарії до 2020 р. за допомогою центру NCIRC НАТО із забезпеченням безперервного моніторингу і повної оперативної інтеграції в національну мережу NKOMKS (National Coordination and Organizational network for cyber/ICT security (NKOMKS)). Це дає можливість ефективно використовувати розвиток колективного потенціалу реагування на кібер- і гібридні загрози на національному й міжнародному рівнях [10].

Національна координаційна й організаційна мережа із забезпечення кіберзахисту та безпеки інформаційно-комунікаційних технологій (NKOMKS) визначає та вста-

новлює вимоги відносно функціональної сумісності й операційних можливостей щодо запобіганням кіберзагрозам, а також відновленню стабільності в умовах кіберінцидентів. Загалом ця система національної мережі кіберзахисту інформаційного простору виконує досить широкі функції, зокрема:

- моніторинг і створення актуальної і всебічної картини національного кіберпростору;
- забезпечення безперебійної роботи комунікаційних та інформаційних систем;
- координування заходів реагування й оперативної взаємодії під час масових кіберінцидентів.

Забезпечення надійності, безпеки та стійкості NKOMKS покладено на National Cyber Security Coordinator (NCSS), до функцій якого входять:

- моніторинг та оцінювання національного статусу безпеки в інформаційному просторі;
- координація дій і реагування на кіберінциденти;
- організація, забезпечення розвитку Національного Центру Кібер Ситуації (National Cyber Situation Center (NCSC)).

Зауважимо, що на NCSS покладено виконання функцій Секретаря Ради з питань кіберстійкості (SKU) та керівництво розробляннням, упровадженням і моніторингом реалізації Національної стратегії кібербезпеки [31, с. 83–86].

Згідно з Національною Стратегію кібербезпеки, 31 жовтня 2018 р. парламент Болгарії прийняв перший в історії Закон про кібербезпеку (Cyber Security Law Prom. DV. issue 94 of 13 November 2018, amended DV. issue 69 of 4 August 2020, amended and ext. DV. issue 85 of October 2, 2020) [7].

Новий Закон про кібербезпеку набув чинності 13 листопада 2018 р. Основною метою Закону є досягнення високого рівня безпеки там, де задіяна критична інфраструктура, а відповідно збереження безперебійної роботи державного сектора. Окрім того, Законодавство також націлене на цифрові послуги, а саме: має на меті врегулювати організацію, управління та контроль кібербезпеки в Болгарії, у т. ч. шляхом покладення нових важливих зобов'язань щодо підтримки інформаційної та мережної безпеки на постачальників цифрових послуг та операторів основних послуг в енергетиці, транспорті, охороні здоров'я, банківській і фінансовій інфраструктурах.

Указаний Закон передбачає, що міністр оборони повинен проводити державну політику щодо захисту і протидії кібератакам і гібридним впливам на системи зв'язку й інформації, системи управління країною та збройними силами. Міністерство оборони має координувати співпрацю в галузі кіберзахисту з НАТО та ЄС, а разом із Міністерством внутрішніх справ, ДАНС та Державним агентством із питань електронного урядування будуть відповідати за планування й реалізацію заходів щодо підготовки до кіберзахисту та кіберстійкості держави в умовах надзвичайних ситуацій, воєнного стану чи війни. Також задекларовано створення кіберрезерву, який буде використано для наукового й освітнього потенціалу країни. Спеціальні вимоги до безпеки також буде введено для цифрових операторів і провайдерів у Болгарії. Управління системою кібербезпеки покладено на уряд, якому допомагатиме Рада, що складається з представників спецслужб.

Румунія. Законодавство Румунії у сфері кіберзахисту базується на таких основних документах.

Рішення № 271/2013 про затвердження Стратегії кібербезпеки Румунії та Плану дій на національному рівні щодо впровадження Національної системи кібербезпеки (Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică) [11].

Рішення від 11.05.2011 № 494 про створення Національного центру реагування на випадки кібербезпеки – CERT-RO (Hotarare Nr. 494 din 11.05.2011 privind înfiinţarea Centrului Naţional de Răspuns la Incidente de Securitate Cibernetică – CERT-RO). [12]

Закон № 362 від 28 грудня 2018 р. щодо забезпечення високого загального рівня безпеки комп'ютерних мереж і систем (Legea nr. 362 din 28 decembrie 2018 privind asigurarea unui nivel comun ridicat de securitate a retelelor si sistemelor informatice) [14].

Національну стратегію забезпечення кібербезпеки Румунії (2013) (Romania's Cyber Security Strategy and the National Action Plan on Implementation of the National Cyber Security (2013)) [19] прийнято 2013 р. Це перша і єдина на сьогоднішній день стратегія кібербезпеки Румунії. Уряд Румунії прийняв Cybersecurity Strategy of Romania (CSR) у відповідь на регуляторний процес щодо питань кіберзахисту, а також дотримання та виконання Постанови Уряду Румунії № 486 від 2011 р. про створення CERT-RO.

CSR пояснює контекстні межі кібербезпеки в Румунії, зокрема це: швидкий розвиток інформаційно-кумунікаційних технологій (ІКТ), а також переваги діджиталізації та пов'язані з нею вразливості. Мета CSR полягає у захисті національних інтересів у площині кібербезпеки, причому з урахуванням цілей Національної стратегії захисту критичної інфраструктури та Стратегії Національна оборонна 2020–2024 (National Defense Strategy 2020–2024 (NDS)) [21]. CSR визначає цілі, які значною мірою зосереджено на створенні інтегрованої Національної системи кібербезпеки (National Cyber Security System (NCSS)) для здійснення всіх заходів щодо запобігання та реагування на кібератаки та кіберінциденти. Окрім того, Стратегія у своїх цілях підкреслює розвиток співпраці в межах ЄС і НАТО, щодо єдиних стандартів у питаннях кіберзахисту.

Разом із тим національна стратегія кібербезпеки передбачає, що Румунія забезпечує функціонування динамічного інформаційного середовища на основі функціональної сумісності й послуг, характерних для інформаційних суспільств, а також забезпечує відповідальність основних прав і свобод громадян та інтересів національної безпеки у відповідних правових межах.

Як зауважує Т. Ткачук, з метою забезпечення кібербезпеки Румунії, Стратегія визначає такі цілі: адаптація нормативного й інституціонального підґрунтя до динаміки конкретних загроз у кіберпросторі; установлення й застосування мінімальних профілів і вимог безпеки для національних кіберсистем, що забезпечують правильну роботу критичної інфраструктури; забезпечення стійкості кіберінфраструктури; використання можливостей кіберпростору для просування інтересів, цінностей і національних цілей у кіберпросторі; сприяння та розвиток міжнародного співробітництва у сфері кібербезпеки; активна участь в ініціативах міжнародних організацій, учасницею яких є Румунія, в межах реалізації комплексу заходів щодо зміцнення довіри до міжнародного використання кіберпростору [26, с. 62–72].

Особливу увагу Національна стратегія забезпечення кібербезпеки Румунії (2013) приділяє розвитку національних можливостей щодо управління ризиками у сфері кібернетичної безпеки.

Окрім того в Румунії діє Національна стратегія щодо цифрового порядку денного для Румунії 2020 (National Strategy on the Digital Agenda for Romania 2020). Вона затверджена урядом Румунії у лютому 2015 р. й узгоджується з європейською політикою, викладеною у до-

кументі під назвою Цифрова програма для Європи 2010 (Digital Agenda for Europe of 2010). Цифрова програма Румунії адаптована до національних інтересів Румунії в контексті національної стратегії безпеки на період 2015–2020 рр. Зокрема, NSDAR забезпечує розвиток інформайційно-комунікаційних технологій (ІКТ) у Румунії відповідно до стандартів ЄС і подальшої інтергації Румунії до єдиного цифрового ринку ЄС. У документі викладено чотири напрямки (сфери) діяльності, зокрема:

1) електронне урядування, функціональна сумісність, кібербезпека, хмарні обчислення та соціальні медіа;

2) ІКТ у галузі освіти, культури й охорони здоров'я;

3) ІКТ в електронній комерції та дослідженнях, розвиток та інновації в ІКТ;

4) широкосмугова та цифрова інфраструктури послуги: зусилля із забезпечення соціальної інтеграції [16].

Також у національній системі кіберзахисту діє Національна оборонна стратегія 2020–2024 (National Defense Strategy 2020–2024, 2020 (NDS)), під назвою "Разом за безпечну та процвітаючу Румунію у світі, позначеному новими викликами" ("Together, for a safe and prosperous Romania in a world marked by new challenges"). Вона базується на документах, зокрема: Law of National Security of Romania (1991), Law of National Defense of Romania (1994), Romania's National Security Strategy (2001), White Paper on Government Security, the National Defense, the Law on the Planning of the National Defense of Romania (2004) [21].

Стратегія Національної оборони Румунії опублікована в липні 2020 р. Це друга стратегія оборони – після оборонної стратегії 2015 р. (National Defense Strategy 2015–2019), яка розглядає зміну парадигми в національній обороні та безпеці, що відображає зростаючу складність, взаємозв'язок і непередбачуваність динаміки загального середовища безпеки, а також потенційну глобальну реконфігурацію влади. Окрім того, ця стратегія робить акцент на використанні кібернетичних можливостей у контексті геополітики та війни. Стратегія національної оборони 2020–2024 зосереджена на забезпечення національної безпеки й підвищення стійкості румунського суспільства та його критичної інфраструктури проти можливих криз. Вона виокремлює проблеми, пов'язані з інформаційним простором, а саме з використанням кіберпрограм, зокрема: швидкий розвиток інформаційно-комунікаційних технологій і глобалізація взаємозв'язку породжують новий тип загроз і вразливостей, що виникають у звязку з використанням новітніх технології, таких як: Cryptocurrencies, Blockchain, 5G–Network, Artificial intelligence, Machine learning, Internet of Things, Big Data, Quantum technology, Darknet, Cloud technology, Neural Network. Стратегія визнає, що кіберзагрози можуть мати асиметричну та гібридну форми, особливо стосовно терористичної діяльності, кіберзлочинності й інформаційних операцій. Нарешті, оборонна стратегія, у межах своїх напрямків діяльності виділяє пріоритетні заходи для пом'якшення згаданих вище кіберзагроз і ризиків. Але в Стратегії не розглядають варіанти того, як Румунія може відповісти на серйозну кібератаку.

Провідну роль у забезпеченні кібербезпеки Румунії відведено її спеціальному контррозідувальному органу, Румунській службі інформації, у структурі якої створено національний центр кібербезпек. Головною функцією цього центру є поєднання систем технічного захисту із можливостями спецслужби з метою отримання інформації, необхідної для попередження, припинення та подолання наслідків кібератак на інформаційно-телекомунікаційні системи об'єктів критичної інфраструктури держави.

Для забезпечення інформаційної безпеки і зокрема протистояння кіберзагрозам у Румунії створено CERT-RO – національну команду комп'ютерного реагування на надзвичайні ситуації. Вона охоплює всіх користувачів румунських мереж. CERT-RO – національний CERT Румунії, створений як незалежна урядова структура для досліджень, розроблення та здійснення експертиз у галузі кібербезпеки. Це спеціалізована організація, відповідальна за запобігання, аналіз, виявлення та реагування на кіберінциденти. Також CERT-RO відповідає за розроблення та розповсюдження публічної політики для запобігання та протидії інцидентам, що трапляються в національній кіберінфраструктурі. Окрім того CERT-RO має право залагоджувати всі типи інцидентів комп'ютерної безпеки, які трапляються або загрожують виникнути в румунському кіберпросторі. У червні 2020 р. опубліковано RFC 2350 description for CERT-RO (Romanian National Computer Emergency Response Team), в якому визначено функції та завдання національної команди комп'ютерного реагування на надзвичайні ситуації.

CERT-RO є учасником FIRST та TF-CSIRT, а також спілкується та співпрацює з іншими CSIRT, на основі обміну відповідною інформацією, і діє в межах, установлених румунським та європейським законодавством.

Щоб узгодити свою політику в галузі кібербезпеки з ЄС і НАТО уряд Румунії розробив Пропозиції щодо Закону про кібербезпеку (Legea privind securitatea cibernetică, 2014) [12]. Цей законопроект було подано до Парламенту, який прийняв його в грудні 2014 р. Однак Конституційний суд повністю скасував закон про кібербезпеку у січні 2015 р., оскільки він порушував деякі положення, що містяться щонайменше у восьми статтях Конституції Румунії. Широкі можливості (PCL) прагнули розширити регулятивні повноваження щодо всіх юридичних осіб, які використовують ІКТ. Більше того, урядовим органам, зокрема румунській Службі розвідки, надавався доступ до систем ІКТ та журналів провайдерів хостингу даних без додаткового попереднього юридичного дозволу. Насамкінець, PCL підняла RIS до статусу національного органу з питань кібербезпеки і надала агенції провідну роль у питаннях кіберзахисту. З 2015 р. PCL переглядались кілька разів, але все ще не прийняті [20].

Словаччина. Словацька Республіка вперше розробила концептуальну основу своєї кібербезпеки 2008 р. 2015 р. у Словаччині прийнято два документи: Концепція кібербезпеки Словацької Республіки на 2015–2020 рр. (Cyber Security Concept of the Slovak Republic for 2015–2020 (2015)) [6] , і План дій із Концепції кібербезпеки Словацької Республіки на 2015–2020 рр. (Action Plan for the Implementation of the Cyber Security Concept of the Slovak Republic for 2015-2020) [3]. Національна Рада Словацької Республіки 30.01.2018 р. прийняла Закон про кібербезпеку та про внесення змін і доповнень до деяких актів (Slovak Cyber Security Act (Act No. 69/2018 Coll., the "Act") [1]. Словацький Закон про кібербезпеку вступив у силу з квітня 2018 р. Новий Закон транспонує у словацьку правову систему частину законодавства Європейського Союзу про кібербезпеку, зокрема і Директиву про безпеку мережних та інформаційних систем. Цей законодавчий акт передбачає правові заходи для підвищення загального рівня кібербезпеки держави. Закон про кібербезпеку застосовується як до державного, так і до приватного секторів Словаччини, і його основною метою є застосування стратегії боротьби з кіберзагрозами. Дотримання Закону про кібербезпеку контролює Управління національної безпеки (National Security Authority (NBU)), що виступає в ролі національної групи реагування на випадки комп'ю-

терної небезпеки. NBU також відповідає за підготовку національної стратегії кібербезпеки. Поточні стратегічні документи, що стосуються кібербезпеки, містять Концепцію кібербезпеки Словацької Республіки на 2015–2020 рр., затверджену урядом Словаччини відповідно до Резолюції No. 328/2015, та План заходів щодо реалізації Стратегії кібербезпеки Словацької Республіки на 2015–2020 рр. затверджений урядом Словаччини відповідно до резолюції No. 93/2016. Хоча перший стратегічний документ пропонує нову інституційну базу кібербезпеки, останній пропонує завдання, які мають бути забезпечені для забезпечення належного захисту кіберпростору держави від потенційних небезпек, що можуть завдати непоправної шкоди Словацькій Республіці.

Питаннями управління секретною інформацією і взагалі інформаційною безпекою, зокрема й кібербезпекою займається безпосередньо Служба національної безпеки Словаччини, Міністерство оборони безпосередньої ролі в управлінні національної кібербезпекою не відіграє. А взаємному обміну інформацією сприяє Комітет із питань інформаційної безпеки Міністерства фінансів, який виконує консультативну та координуючу роль, готуючи стратегічні та технічні матеріали щодо інформаційної безпеки. Деякі конкретні теми контролюють Рада Безпеки, Міністерство внутрішніх справ і Міністерство оборони.

Agnija Tumkevič зазначає, що Словацька стратегія кібербезпеки на державному рівні – це система, яка включає прийняття та застосування ефективних заходів контролю ризиків техніко-організаційного характеру в кіберпросторі. Окрім того вона базується на постійному і плановому підвищенні політичної, правової, економічної, безпекової, оборонної й освітньої обізнаності. Цікавим є той факт, як зазначає автор, у документі відсутня будь-якої цілісної, формальної термінології кібербезпеки. Як підкреслюють автори, це означає, що проблеми кібербезпеки не є ізольованими лише Словацькою Республікою і не обмежуються одним або кількома сегментами соціально-політичного середовища, а розглядаються глобально, зокрема в контексті створення уніфікованої нормативно-правової площини забезпечення кіберзахисту [28, с. 73–88].

Словацька стратегія підкреслює відповідність принципам кібербезпеки, викладеним у документах ЄС і НАТО. Разом із тим вона базується на національній законодавчій основі, включаючи положення щодо оборонного планування, планування кризових ситуацій і координації розвідувальних служб.

Як учасник НАТО та ЄС, Словаччина бере участь у розробці міжнародних стратегічних документів, які формують ефективну нормативно-правову основу кібербезпеки. Відповідно це означає, що Словаччина трансформує міжнародні правові документи у свою національну законодавчу базу у сфері забезпечення інформаційної безпеки і зокрема в питання кібернетичного захисту. У цьому уряд Словаччини тісно співпрацює із Центром передового досвіду кібернетичної оборони НАТО в Таллінні, а також з Європейським агентством із питань мережної роботи й інформаційної безпеки (ENISA) та Європейським центром кіберзлочинності (EC3), який створено 2013 р.

Як зазначає Marek Gorka, політика кібербезпеки складається з декількох ключових заходів. Перший із них – це створення інституційної бази для управління кібербезпекою. Другий – створення та прийняття правової бази щодо забезпечення кібербезпеки. Третій – підтримка та застосування основних систем безпечного адміністрування кібернетичного простору. Четвертий – підтримка, підготовка та впровадження системи освіти з кібербезпеки. П'ятий – запровадження та застосування системи контролю ризику зв'язку серед зацікавлених сторін. Шостий – активне міжнародне співробітництво, і насамкінець сьомий – підтримка науки та досліджень, пов'язаних із кібербезпекою [33, с. 75–98]

Профілактика є ключовим моментом у стратегії кібербезпеки, яка передбачає використання захисних інструментів, що запобігатимуть кіберзагрозам. У цьому контексті в центрі уваги не тільки громадська освіта, але й розвідувальні заходи, які збирають та оцінюють дані розвідки з метою прогнозування та запобігання певним кіберінцидентам. Цей документ демонструє систему реагування на існуючі або потенційні загрози, тобто кроки, ужиті для ефективного реагування на конкретні події. У той самий час вона окреслює механізм усунення наслідків кризової ситуації та повернення до стабілізованого стану, який має зменшити шкоду, заподіяну кібератаками.

Хорватія. У Хорватії ще з 2007 р. діє закон про інформаційну безпеку Information Security Act of the Republic of Croatia). Цим законодавчим актом визначено поняття інформаційної безпеки, її елементи, заходи забезпечення і стандарти, а також функціональні компетентності органів для прийняття й реалізації рішень у сфері протидії загрозам та забезпеченні інформаційної безпеки держави. Реалізація державної політики у сфері забезпечення інформаційної безпеки відповідно до цього законодавчого акта покладається на Управління Ради національної безпеки (NSA) (Office of the National Security Council – UVNS), Бюро з безпеки інформаційних систем (NCSA) (Information Systems Security Bureau – ZSIS), а також національний орган із питань профілактики й захисту від комп'ютерних загроз систем суспільної інформації Республіки Хорватія (CERT).

Бюро безпеки інформаційних систем (ISSB) є центральним державним органом, відповідальним за технічні сфери інформаційної безпеки державних органів Республіки Хорватія. Структура й обов'язки Бюро безпеки інформаційних систем регулюються Законом про систему безпеки й розвідки Республіки Хорватія (Security and Intelligence System Act of the Republic of Croatia) [36], Законом про інформаційну безпеку (Information Security Act of the Republic of Croatia) [30] та Положенням про заходи інформаційної безпеки Республіки Хорватія (Regulation on Information Security Measures of the Republic of Croatia) [35].

Відповідно до законодавства Хорватії, Бюро безпеки інформаційних систем поряд з акредитацією безпеки інформаційних систем уповноважене на здійснення заходів, пов'язаних з управлінням криптоматеріалами, що використовують під час обміну секретною інформацією між державними органами та зарубіжними країнами, для проведення дослідження, розробляння та тестування технологій захисту класифікованих даних та видачі сертифікатів на їхнє використання. Поряд із запобіганням і реагуванням на загрози комп'ютерній безпеці, Бюро безпеки інформаційних систем несе відповідальність за регулювання технічних сфер стандартів безпеки інформаційних систем у всіх постановах та їхнє постійне пристосування до міжнародних стандартів і рекомендацій. Бюро безпеки інформаційних систем бере участь у національній стандартизації сфер безпеки інформаційних систем.

Акредитацію безпеки інформаційних систем проводить Бюро безпеки інформаційних систем у співпраці з Управлінням Ради національної безпеки, запобігання та реагування на загрози комп'ютерній безпеці, а створення рекомендацій і стандартів щодо захисту інформаційних систем – у співпраці з Національним CERT.

Управління Ради національної безпеки (UVNS) виконує експертні й адміністративні завдання для Ради національної безпеки та Ради з питань координації служб безпеки та розвідки, а також завдання, які дозволяють Президенту Республіки й Уряду здійснювати контроль за роботою органів безпеки та розвідки. UVNS також є органом національної безпеки Хорватії, який координує, узгоджує прийняття та контролює виконання заходів і стандартів інформаційної безпеки в Республіці Хорватія.

Національний CERT (CERT.hr) – це відділ Хорватської академічної та дослідницької мережі – CARNET, який був створений відповідно до Закону про інформаційну безпеку Республіки Хорватія. Згідно із цим Законом, CERT.hr є національним органом із запобігання кіберзагрозам та захисту безпеки громадських інформаційних систем у Республіці Хорватія (Information Security Act of the Republic of Croatia). Основним завданням департаменту є управління інцидентами комп'ютерної безпеки для збереження безпеки інформаційних систем у Хорватії. Відділ CERT.hr займається інцидентами, якщо одна зі сторін інциденту перебуває в Республіці Хорватія, за винятком державних органів, які підпадають під дію інформаційних систем Бюро безпеки (ZSIS).

На додаток до контролю за здійсненням Стратегії та її Плану дій на ці міжвідомчі органи покладено певні завдання, пов'язані з управлінням у кіберкризах.

2015 р. у Хорватії прийнято національну стратегію кібербезпеки (National Cyber Security Strategy of the Republic of Croatia) [15], яка є частиною стратегії оборони, що є сферою відповідальності Міністерства оборони Хорватії. Стратегія кібербезпеки Хорватії, як зазначає Т. Ткачук, базується на таких принципах: усебічність підходу до кібербезпеки, що охоплює кіберпростір, інфраструктуру й користувачів відповідно до хорватської юрисдикції; інтеграція заходів у різних сферах забезпечення кібербезпеки; проактивність унаслідок постійного коректування заходів і періодичне коригування їхніх стратегічних кордонів; зміцнення стійкості, надійності і керованості шляхом застосування універсальних критеріїв конфіденційності, цілісності й доступності певних груп інформації; постійне вдосконалення правової бази; субсидіарність у розподілі повноважень [25, с. 104–110].

Чехія. У Чеській Республіці Національну стратегію інформаційної безпеки вперше опубліковано 2005 р. У ній піднімались питання регулювання безпеки у кіберпросторі.

2011 р. кібербезпеку визначено як одне з головних і пріоритетних завдань Чеського уряду, а кіберзагрози прирівняно до найсерйозніших загроз безпеки у площині розвитку інформаційного суспільства.

Урядом Чехії 2015 р. затверджено Стратегію кібербезпеки Чеської Республіки на період до 2020 р. (Cyber Security Strategy of the Czech Republic 2015–2020 (2015)) [5], яка спрямована на захист систем інформаційно-комунікаційних технологій і мінімізацію збитку, викликаного кіберзлочинами. У тому свмому 2015 р. Уряд Чехії затвердив оновлену Стратегію національної безпеки, де підкреслюються наростаючі проблеми Чеської Республіки, а також інших країн НАТО та Європейського Союзу, викликані кризою системи міжнародної безпеки. Стратегія кібернетичної оборони Чехії відповідає на всі ключові проблеми у цій сфері.

Розроблений документ відповідає Плану дій із національної стратегії кібербезпеки на період 2015–2020 рр. (National Cyber Security Strategy of the Czech Republic for the period from 2015 to 2020) [2], затвердженому Урядом Чеської Республіки 25 травня 2015 р. У цьому документі уряд доручив Військовій розвідці створити центр, здатний виконувати широкий спектр операцій у кіберпросторі на підтримку зовнішніх операцій НАТО і ЄС, а також у разі гібридного конфлікту для захисту Чеської Республіки.

Відповідно до стратегії кібербезпеки Чехії, сучасні кібертехнології є ключовим викликом для держави, що має особливі наслідки для будь-яких державних організацій, які залежать від інформаційних і комунікаційних засобів. Цей документ підкреслює критичну роль інформаційної безпеки, утрата якої може мати непередбачувані наслідки для суспільства. У стратегії зазначено, що кібербезпека має йти разом із захистом основних прав і свобод людини та принципів демократичної держави. У зв'язку із цим відкрито і нейтральний характер інтернету, закони про свободу вираження поглядів і конфіденційність гарантують захист громадянських свобод у кіберпросторі.

Marek Gorka зазначає, що ще одним важливим елементом стратегії є класифікація загроз, що виникають через кіберпростір. До таких загроз належать кібернетичне шпигунство (політичне, військове, промислове тощо), кіберзлочинність, хактивізм, дезінформація та кібертероризм. У контексті цього автор виділив чотири основні частини Чеської стратегії кібербезпеки: перша пропонує бачення кібербезпеки держави із цілями, що виходять за визначений термін 2015–2020 рр. У другій частині викладено основні принципи, які мають формувати політику кібербезпеки. Третій визначає конкретні проблеми в галузі кібербезпеки для держави та міжнародних організацій, а четвертий описує стратегічні цілі, досягнення яких є визначальними для політики Чеської кібербезпеки в цей період. У документі також наголошено на зобов'язаннях держави внаслідок її ролі в міжнародних організаціях і колективних оборонних структурах НАТО [33, с. 75–98].

У серпні 2017 р. у Чеській Республіці створено Національне агентство (бюро) з кібернетичної та інформаційної безпеки (NUKIB) (National Cyber and Information Security Agency (NUKIB)). Воно було створено на підставі Закону № 205/2017 Coll. "Про внесення змін до Закону № 181/2014 Coll. "Про кібербезпеку і поправки до відповідних законів"" (Act No. 205/2017 Coll., Amending Act No. 181/2014 Coll., on cybersecurity and on amendments to related acts). Національне агентство (бюро) з кібернетичної й інформаційної безпеки є центральним органом державного управління з питань кібербезпеки. До компетенції цієї структури входить запобігання кіберзагрозам проти елементів критичної інформаційної інфраструктури, базових інформаційних систем обслуговування, проти важливих інформаційних систем і вибраних інформаційних систем державного управління, а також захист секретної інформації в галузі інформаційно-комунікаційних систем і криптографічного захисту. Основні напрямки діяльності агенції: функціонування урядового CERT (GovCERT.CZ); співпраця з національними та міжнародними командами CERT та CSIRT; розробляння стандартів безпеки для інформаційної системи CII / IIS; дослідження, розробляння та впровадження новітніх технологій у галузі кібербезпеки; оцінювання ризиків кібербезпеки та вжиття відповідних коригувальних і профілактичних заходів; захист секретної інформації в галузі інформаційно-комунікаційних систем; криптографічний захист; функціонування Національної служби підтримки PRS, яка є однією зі служб європейської супутникової системи Galileo (NCPRS);

Виконавчим відділом Національного агентства з питань кібернетичної та інформаційної безпеки, який забезпечує безпосереднє виконання визначених напрямків діяльності, є Національний центр кібербезпеки

(NCKB). Національний центр кібербезпеки контролює діяльність групи урядового CERT (GovCERT.CZ), а також наукові дослідження та розробки в області кіберзахисту; працює над усуненням кіберзагроз важливим елементам критичної інфраструктури та важливим інформаційним системам державного управління; управляє та координує залагодження інцидентів кібербезпеки на важливих елементах критичної інфраструктури; представляє Чеську Республіку в органах міжнародних установ із кібербезпеки.

Agnija Tumkevič зазначає, що загальна відповідальність за національну кібербезпеку Чехії покладається на Національний орган безпеки. Національний центр кібербезпеки – агентство, яке діє в межах Національної служби безпеки, є частиною національної та міжнародної системи раннього попередження. Крім того, Міністерство внутрішніх справ просуває проблеми кібербезпеки на політичному рівні, тоді як Міністерство оборони займається лише питаннями кібербезпеки спільно з НАТО [28, с. 73–88].

З 2017 р. у Чехії функціонує Центр боротьби з тероризмом і гібридними загрозами. Центр підпорядкований Міністерству внутрішніх справ Чехії, його основні завдання – спостереження за підозрілими публікаціями в інтернеті, викриття "фейкових новин" із метою перешкоджання їхньому широкому поширенню, боротьба проти "пропаганди зовнішніх сил".

2018 р. Міністерство оборони Чехії оголосило, що "Національний центр кібероперацій (NCKO) розробив стратегію кіберзахисту Чеської Республіки на період 2018–2022 (Strategie kybernetické obrany ČR 2018–2022) [17], яка встановлює політичні умови для національної оборони в кіберпросторі і відповідає положенням Плану дій із національної стратегії кібербезпеки на період 2015–2020 рр., затвердженому Урядом Чеської Республіки 25 травня 2015 р.

ВИСНОВКИ. Оскільки кібератаки та зовнішні кіберзагрози як правило мають дестабілізуючий характер, то країни ЄС формують свою політику безпеки на основі міжнародній співпраці в т. ч. з Єврпейськими інституціями, інтегруючи свої національні ресурси кіберзахисту в межах вимог права Європейського Союзу. Зазначимо, що співпраця держав-членів ЄС зі спеціальними інституціями Європейського Союзу носить обмежений характер, оскільки інформація щодо національних критичних структур має статус секретної й охороняється національними законодавствами. Водночас, наявна архітектура кіберпростору в державах ЄС, зокрема в Болгарії, Румунії, Словаччині, Чехії та Хорватії, а також відсутність уніфікованої правової платформи щодо забезпечення інформаційної безпеки, зокрема захисту критично-важливої інфраструктури від кібератак, є основною проблемою під час створення дієвих і ефективних механізмів забезпечення національної безпеки країн ЄС і безпеки Європейського Союзу в цілому. Таке відношення диктує застосування насамперед силових механізмів щодо протидії кіберзлочинності, як найбільш ефективних в умовах трансформації сучасної системи міжнародної безпеки.

Таким чином, нові країни Європейського Союзу активно модернізують власні сектори безпеки у кіберпросторі відповідно до права ЄС. Цей процес відбувається шляхом упорядкування нормативної бази, що має забезпечити цілісність державної політики у вказаній сфері, а також вироблення єдиних принципів щодо забезпечення стійкості і стабільності інформаційного простору. Зважаючи на досвід зазначених країн у формуванні національної системи кіберзахисту, Україна повинна стати активним учасником усіх безпекових процесів в Європі, а також активувати процес створення власних сил швидкого реагування на кіберзагрози. Це буде платформою формування організаційно-правової основи забезпечення національної кібербезпеки України у контексті адаптації вітчизняного законодавства до стандартів права ЄС у цій сфері.

Наведені вище законодавчі кроки країн Європейського Союзу (Болгарії, Румунії, Словаччини, Хорватії та Чехії) яскраво підтверджують, що у цих країнах питанням інформаційної безпеки приділяється особлива увага. А практичний досвід цих держав особливо важливий у формуванні національної нормативно-правової бази України у сфері забезпечення інформаційної безпеки. Відповідно адаптація правових стандартів, що мають місце в державах-членах ЄС у цій сфері, є пріоритетним напрямком нашої держави в контексті розбудови національної системи інформаційної безпеки. Таким чином необхідно активно охороняти свій інформаційний простір і приділяти першочергову увагу захисту критично важливої інфраструктури як ключової умови національної безпеки. Така тенденція зможе підняти інформаційну безпеку до рівня національної безпеки і зосередитись на захисті державних ресурсів інформаційно-комунікаційних технологій. Власне такий формат забезпечення інформаційної безпеки в контексті кіберзахисту диктує силовий підхід, як найефективніший.

Список використаних джерел

1. Act on Cybersecurity and on Amendments and Supplements to certain Acts of January 30, 2018 URL: https://www.nbu.gov.sk/wp-content/uploads/legislativa/EN/Act_Cybersecurity.pdf (дата звернення: 03.03.2021)

2. Action Plan for the National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020 URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf (дата звернення: 05.03.2021)

3. Action Plan for the Implementation of the Cyber Security Concept of the Slovak Republic for 2015-2020 URL:https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ActionPlanforthe ImplementationoftheCyberSecurityConceptoftheSlovakRepublicfor20152020_3_.pdf (дата звернення: 03.03.2021)

4. Bulgarian National Cyber Security Strategy URL:https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2016/Cybersecurity%20Forum%20Bulgaria/Bulgaria_sharkov_todorov.pdf (дата звернення: 01.03.2021)

5. Cyber Security Strategy of the Czech Republic 2015-2020 (2015) URL:https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf (дата звернення: 05.03.2021)

6. Cyber Security Concept of the Slovak Republic for 2015 – 2020 (2015) URL:https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1 (дата звернення: 03.03.2021)

7. Cyber Security Law Prom. DV. issue 94 of 13 November 2018, amended DV. issue 69 of 4 August 2020, amended and ext. DV. issue 85 of October 2, 2020 URL: https://lex.bg/bg/laws/ldoc/2137188253 (дата звернення: 01.03.2021)

8. Communication From The Commission To The Council, The european Parliament, The European Economic And Socialcommittee And The Committee Of The Regions "Network and Information Security:Proposal for a European Policy Approach" URL:https://www.academia.edu/22286875/Network_and_Information_Security_Proposal_for_a_European_Policy_Approach_Network_and_Information_Security_Proposal_for_a_European_Policy_Approach (дата звернення: 06.03.2021)

9. Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" URL:https://ifap.ru/pr/2009/n090331a.pdf (дата звернення: 06.03.2021)

10. Програма за развитие на отбранителните способности на Въоръжените сили на Република България 2020 и за определяне числеността на въоръжените сили, приета с Решение на Народното събрание от 25.11.2015 г., публикувано в Държавен вестник, бр.93, от дата 1.12.2015 URL: https://www.mod.bg/bg/doc/cooperation/20181009_Programa_razvitie_otbranit%20sposobnosti.pdf (дата звернення: 01.03.2021)

11. Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică URL: https://lege5.ro/Gratuit/gm3demzrgq/hotararea-nr-271-2013-pentru-aprobarea-strategiei-de-securitate-cibernetica-a-romaniei-si-a-planului-

de-actiune-la-nivel-national-privind-implementarea-sistemului-national-de-securitate-cibernetica (дата звернення: 02.03.2021)

12. Hotarare Nr.494 din 11.05.2011 privind înfiinţarea Centrului Naţional de Răspuns la Incidente de Securitate Cibernetică – CERT-RO URL: https://cert.ro/vezi/document/hg-494-2011-infiintare-cert (дата звернення: 10.04.2021)

13. Information Technology Security Evaluation Criteria (ITSEC), Provisional Harmonised Criteria, June 1991 URL: https://www.ssi.gouv.fr/uploads/2015/01/ITSEC-uk.pdf (дата звернення: 06.03.2021)

14. Legea nr. 362 din 28 decembrie 2018 privind asigurarea unui nivel comun ridicat de securitate a retelelor si sistemelor informatice URL: http://legislatie.just.ro/Public/DetaliiDocument/209670 (дата звернення: 02.03.2021)

15. National Cyber Security Strategy of the Republic of Croatia URL: https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf (дата звернення: 04.03.2021)

16. National Strategy on the Digital Agenda for Romania 2020 URL: https://gov.ro/en/government/cabinet-meeting/national-strategy-on-the-digital-agenda-for-romania-2020 (дата звернення: 02.03.2021)

17. Národní centrum kybernetických operací (NCKO) vypracovalo Strategii kybernetické obrany České republiky pro období 2018 – 2022 URL: https://www.mocr.army.cz/informacni-servis/zpravodajstvi/narodni-centrum-kybernetickych-operaci-vypracovalo-strategii-kyberneticke-obrany-cr-201906/ (дата звернення: 05.03.2021)

18. Report of the Human Rights Committee Volume II General Assembly Official Records Fifty-fifth Session Supplement No. 40 (A/55/40) URL: https://www.refworld.org/docid/3f475a844.html (дата звернення: 06.03.2021)

19. Romania's Cyber Security Strategy and the National Action Plan on Implementation of the National Cyber Security (2013) URL:https://www.cert.ro/vezi/document/strategia-de-securitate-cibernetica (дата звернення: 02.03.2021)

20. Romania's National Cybersecurity and Defense Posture. Cyberdefense Report. Policy and Organizations. Center for Security Studies (CSS), ETH Zürich, Zürich, October 2020

21. The National Defence Strategy for 2020-2024 was approved by Decision no. 22 of the Joint Meeting of the Senate and Chamber of Deputies on June 30th, 2020, and was published in the Official Journal of Romania, Part I, no. 574 of July 1st 2020. URL: https://www.presidency.ro/files/userfiles/National_Defence_Strategy_2020_2024.pdf (дата звернення: 02.03.2021)

22. Treaty Of Lisbon Amending The Treaty On European Union And The Treaty Establishing The European Community (2007/C 306/01) URL:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12007L%2FTXT (дата звернення: 10.04.2021)

23. Климчук О.О., Ткачук Н.А. Роль і місце спецслужб та правоохоронних органів провідних країн світу в національних системах кібербезпеки. Інформаційна безпека людини, суспільства, держави. 2015. № 3 (19). С.75-83

24. Панченко В.М. Зарубіжний досвід формування систем захисту критичної інфраструктури від кіберзагроз. Інформаційна безпека людини, суспільства, держави 2012. № 3 (10) С.91-100

25. Ткачук Т. Ю. Забезпечення інформаційної безпеки у країнах центральної Європи. Юридичний науковий електронний журнал. 2017 № 5. Ст.106 http://lsej.org.ua/index.php/arkhiv-nomeriv?id=80 (дата звернення:04.03.2021)

26. Ткачук Т.Ю. Забезпечення інформаційної безпеки: досвід окремих країн східної Європи. *Інформація і право.* 2017. № 4 (23). С. 62-72

27. Ткачук Т. Ю. Інформаційна безпека держави у національному законодавстві європейських країн. Visegrad Journal on Human Rights. 2018. № 1. С. 145–150.

28.Agnija Tumkevič . Cybersecurity in Central Eastern Europe: from identifying risks to countring threats. BALTIC JOURNAL OF POLITICAL SCIENCE. 2016. December 2016, № 5 С.73-88.

29. Cian C Murphy and Diego Acosta Arcarazo, 2014. Rethinking Europe's Freedom, Security and Justice. In: Cian C Murphy and Diego Acosta Arcarazo ed. 2014. *EU Security and Justice Law. After Lisbon and Stockholm*, Oxford and Portland, Oregon: Hart Publishing, pp.1-17.

30. Information Security Act, passed by the Croatian Parliament at its session on 13 July 2007. URL: https://www.zsis.hr/UserDocsImages/Sigurnost/Security/Information%20Security%20Act.pdf (дата звернення: 04.03.2021)

31. Dimitrov N., Valentin Najdenov. National Security in Bulgaria – is it really a system? International Scientific Journal "Security & Future". 2019, pp.83-86.

32. László Kovacs. Cyber Security Policy and Strategy in the European Union and NATO. Land Forces Academy Review Vol. XXIII, No 1(89), 2018 pp.16-24.

33. Marek Gorka, 2018. The Cybersecurity Strategy of the Visegrad Group Countries. *Politics in Central Europe* 14(2), pp.75-98.

34. Raphael Bossong, 2018. Intelligence Support for EU Security. Options for Enhancing the Flow of Information and Political Oversinght. SWP Comment 2018/C51, December 2018, 8 pp.1-8.

35. Regulation on information security measures of the Republic of Croatia 2007 URL: https://www.zsis.hr/UserDocsImages/Sigurnost/Security/Regulation%20on%20information%20security%20measures.pdf (дата звернення: 04.03.2021)

36. Security and intelligence System Act of the Republic of Croatia, enacted by the Croatian Parliament at its session on 30 June 2006. URL:https://www.zsis.hr/UserDocsImages/Sigurnost/Security/Security%20and%20Intelligence%20System%20Act.pdf (дата звернення: 04.03.2021)

37. Sevdalina Dimitrova, Stoyko Stoykov, Yosif Kochev. National Cybersecurity Strategies in Member States of the European Union. Administrattiva un Kriminala Justicija. 2015. № 4. pp. 54–58

38. Udo Helmbrecht, 2018. Adequate and effective cybersecurity: state of play. *Speech by ENISA's Executive Director, Prof. Dr. Udo Helmbrecht – Cybersecurity Conference organised by the Austrian Presidency of the Council of the European Union.* European Union Agency For Network and Information Security Vienna, Austria 3rd December 2018, pp.1-6

References

1. Act on Cybersecurity and on Amendments and Supplements to certain Acts of January 30, 2018 URL: https://www.nbu.gov.sk/wp-content/uploads/legislativa/EN/Act_Cybersecurity.pdf (data zvernennia: 03.03.2021) (in English)

2. Action Plan for the National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020 URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf (data zvernennia: 05.03.2021) (in English)

3. Action Plan for the Implementation of the Cyber Security Concept of the Slovak Republic for 2015-2020 URL:https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ActionPlanfortheImplementationoftheCyberSecurityConceptoftheSlovakRepublicfor20152020_3_.pdf (data zvernennia: 03.03.2021) (in English)

4. Bulgarian National Cyber Security Strategy URL:https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2016/Cybersecurity%20Forum%20Bulgaria/Bulgaria_sharkov_todorov.pdf (data zvernennia: 01.03.2021) (in English)

5. Cyber Security Strategy of the Czech Republic 2015-2020 (2015) URL:https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf (data zvernennia: 05.03.2021) (in English)

6. Cyber Security Concept of the Slovak Republic for 2015 – 2020 (2015) URL:https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1 (data zvernennia: 03.03.2021) (in English)

7. Cyber Security Law Prom. DV. issue 94 of 13 November 2018, amended DV. issue 69 of 4 August 2020, amended and ext. DV. issue 85 of October 2, 2020 URL: https://lex.bg/bg/laws/ldoc/2137188253 (data zvernennia: 01.03.2021)

8. Communication From The Commission To The Council, The european Parliament, The European Economic And Socialcommittee And The Committee Of The Regions "Network and Information Security:Proposal for a European Policy Approach" URL:https://www.academia.edu/22286875/Network_and_Information_Security_Proposal_for_a_European_Policy_Approach_Network_and_Information_Security_Proposal_for_a_European_Policy_Approach (data zvernennia: 06.03.2021) (in English)

9. Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" URL:https://ifap.ru/pr/2009/n090331a.pdf (data zvernennia: 06.03.2021) (in English)

10. Програма за развитие на отбранителните способности на Въоръжените сили на Република България 2020 и за определяне числеността на въоръжените сили, приета с Решение на Народното събрание от 25.11.2015 г., публикувано в Държавен вестник, бр.93, от дата 1.12.2015 URL: https://www.mod.bg/bg/doc/cooperation/20181009_Programa_razvitie_otbranit%20sposobnosti.pdf (data zvernennia: 01.03.2021) (in Bulgaria)

11. Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică URL: https://lege5.ro/Gratuit/gm3demzrgq/hotararea-nr-271-2013-pentru-aprobarea-strategiei-de-securitate-cibernetica-a-romaniei-si-a-planului-de-actiune-la-nivel-national-privind-implementarea-sistemului-national-de-securitate-cibernetica (data zvernennia: 02.03.2021) (in Romania)

12. Hotarare Nr.494 din 11.05.2011 privind înfiinţarea Centrului Naţional de Răspuns la Incidente de Securitate Cibernetică – CERT-RO URL: https://cert.ro/vezi/document/hg-494-2011-infiintare-cert (datazvernennia: 02.03.2021) (in Romania)

13. Information Technology Security Evaluation Criteria (ITSEC), Provisional Harmonised Criteria, June 1991 URL: https://www.ssi.gouv.fr/uploads/2015/01/ITSEC-uk.pdf (data zvernennia: 06.03.2021) (in English)

14. Legea nr. 362 din 28 decembrie 2018 privind asigurarea unui nivel comun ridicat de securitate a retelelor si sistemelor informatice URL: http://legislatie.just.ro/Public/DetaliiDocument/209670 (data zvernennia: 02.03.2021) (in English)

15. National Cyber Security Strategy of the Republic of Croatia URL: https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf (data zvernennia: 04.03.2021) (in English)

16. National Strategy on the Digital Agenda for Romania 2020 URL: https://gov.ro/en/government/cabinet-meeting/national-strategy-on-the-digital-agenda-for-romania-2020 (data zvernennia: 02.03.2021) (in English)

17. Národní centrum kybernetických operací (NCKO) vypracovalo Strategii kybernetické obrany České republiky pro období 2018 – 2022 URL:

https://www.mocr.army.cz/informacni-servis/zpravodajstvi/narodni-centrum-kybernetickych-operaci-vypracovalo-strategii-kyberneticke-obrany-cr-201906/ (data zvernennia: 05.03.2021) (in Czech)

18. Report of the Human Rights Committee Volume II General Assembly Official Records Fifty-fifth Session Supplement No. 40 (A/55/40) URL:https://www.refworld.org/docid/3f475a844.html (data zvernennia: 06.03.2021) (in English)

19. Romania's Cyber Security Strategy and the National Action Plan on Implementation of the National Cyber Security (2013) URL:https://www.cert.ro/vezi/document/strategia-de-securitate-cibernetica (data zvernennia: 02.03.2021) (in Romania)

20. Romania's National Cybersecurity and Defense Posture. Cyberdefense Report. Policy and Organizations. Center for Security Studies (CSS), ETH Zürich, Zürich, October 2020

21. The National Defence Strategy for 2020-2024 was approved by Decision no. 22 of the Joint Meeting of the Senate and Chamber of Deputies on June 30th, 2020, and was published in the Official Journal of Romania, Part I, no. 574 of July 1st 2020. URL: https://www.presidency.ro/files/userfiles/National_Defence_Strategy_2020_2024.pdf (data zvernennia: 02.03.2021) (in English)

22. Treaty Of Lisbon Amending The Treaty On European Union And The Treaty Establishing The European Community (2007/C 306/01) URL:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12007L%2FTXT (data zvernennia: 06.03.2021) (in English)

23. Klymchuk O.O., Tkachuk N.A. (2015). Rol i mistse spetssluzhb ta pravookhoronnykh orhaniv providnykh krain svitu v natsionalnykh systemakh kiberbezpeky [Role of law enforcement bodies and special services in national cyber security systems of leading countries]. Naukovyi zhurnal, seriia "Iurydychni nauky" Informatsiina bezpeka liudyny, suspilstva, derzhavy [Scientific Journal Series "Juridical sciences", Information Security of the Person, Society and State], 19 (3), 75-83 (in Ukrainian).

24. Panchenko V.M. (2012). Zarubizhnyi dosvid formuvannia system zakhystu krytychnoi infrastruktury vid kiberzahroz [Foreign experience in forming the systems of critical infrastructure protection]. Naukovyi zhurnal, seriia "Iurydychni nauky" Informatsiina bezpeka liudyny, suspilstva, derzhavy [Scientific Journal Series "Juridical sciences", Information Security of the Person, Society and State], 10 (3), 91-100 (in Ukrainian).

25. Tkachuk T. Yu. (2017). Zabezpechennia informatsiinoi bezpeky u krainakh tsentralnoi Yevropy [Information security ensuring in the countries of central Europe] Yurydychnyi naukovyi elektronnyi zhurnal [Juridical scientific and electronic journal], 5, 104-110 http://lsej.org.ua/index.php/arkhiv-nomeriv?id=80 (data zvernennia: 04.03.2021) (in Ukrainian)

26. Tkachuk T. Yu. (2018). Zabezpechennia informatsiinoi bezpeky: dosvid okremykh krain skhidnoi Yevropy. [Information security ensuring: experience of individual Eastern European countries. Information and law]. Informatsiia i pravo. [Information and law], 23 (4), 62-72 (in Ukrainian).

27. Tkachuk T. Yu. (2018). Informatsiina bezpeka derzhavy u natsionalnomu zakonodavstvi yevropeiskykh krain [Information security of the state in the national legislation of European countries]. Vyshehradskyi zhurnal z prav liudyny [Visegrad Journal on Human Rights], 1, 145-150 (in Ukrainian).

28.Agnija Tumkevič . Cybersecurity in Central Eastern Europe: from identifying risks to countring threats. BALTIC JOURNAL OF POLITICAL SCIENCE. 2016. December 2016, № 5 С.73-88.

29. Cian C Murphy and Diego Acosta Arcarazo, 2014. Rethinking Europe's Freedom, Security and Justice. In: Cian C Murphy and Diego Acosta Arcarazo ed. 2014. *EU Security and Justice Law. After Lisbon and Stockholm*, Oxford and Portland, Oregon: Hart Publishing, pp.1-17

30. Information Security Act, passed by the Croatian Parliament at its session on 13 July 2007. URL: https://www.zsis.hr/UserDocsImages/Sigurnost/Security/Information%20Security%20Act.pdf (data zvernennia: 04.03.2021) (in English)

31. Dimitrov N., Valentin Najdenov. National Security in Bulgaria – is it really a system? International Scientific Journal "Security & Future". 2019, pp.83-86

32. László Kovacs. Cyber Security Policy and Strategy in the European Union and NATO. Land Forces Academy Review Vol. XXIII, No 1(89), 2018 pp.16-24

33. Marek Gorka, 2018. The Cybersecurity Strategy of the Visegrad Group Countries. *Politics in Central Europe* 14(2), pp.75-98

34. Raphael Bossong, 2018. Intelligence Support for EU Security. Options for Enhancing the Flow of Information and Political Oversinght. SWP Comment 2018/C51, December 2018, 8 pp.1-8

35. Regulation on information security measures of the Republic of Croatia 2007 URL: https://www.zsis.hr/UserDocsImages/Sigurnost/Security/Regulation%20on%20information%20security%20measures.pdf (data zvernennia: 04.03.2021) (in English)

36. Security and intelligence System Act of the Republic of Croatia, enacted by the Croatian Parliament at its session on 30 June 2006. URL:https://www.zsis.hr/UserDocsImages/Sigurnost/Security/Security%20and%20Intelligence%20System%20Act.pdf (datazvernennia: 04.03.2021) (in English)

37. Sevdalina Dimitrova, Stoyko Stoykov, Yosif Kochev. National Cybersecurity Strategies in Member States of the European Union. Administrattiva un Kriminala Justicija. 2015. № 4. pp. 54–58

38. Udo Helmbrecht, 2018. Adequate and effective cybersecurity: state of play. *Speech by ENISA's Executive Director, Prof. Dr. Udo Helmbrecht – Cybersecurity Conference organised by the Austrian Presidency of the Council of the European Union.* European Union Agency For Network and Information Security Vienna, Austria 3rd December 2018, pp.1-6

Received: 02/11/2020
1st revision: 12/04/2021
Accepted: 03/05/2021

S. Kavyn, PhD Student (Law),
I. Bratsuk, PhD (Law), Associate Prof.
Ivan Franko National University of Lviv, Lviv, Ukraine

REGULATORY AND LEGAL IMPLEMANTATION OF CYBER SECURITY AS A COMPONENT OF INFORMATION SECURITY IN THE COUNTRIES OF CENTRAL AND EASTERN EUROPE

In the current conditions of globalization of international relations, the EU and, accordingly, each EU Member State have found themselves in a qualitatively new foreign policy orbit. That is why the creation of an effective and reliable system of information security of the EU and in particular of each European Union countries is extremely important in the transformation of international security and diversification of foreign policy to integrate national information security systems into a single international multi-vector system of information space protection. In this format, comes to the fore in this field the study of the experience of EU member states in this field comes to the fore, in order to adapt the standards that exist in the countries of the European Union in the context of information security.

Today, many EU countries have established national information security networks that are able to quickly accumulate the forces and means of public authorities to counter, in particular, cyber threats, thereby ensuring the national security of their countries. But international cooperation on unified approaches to combating cyber threats in the information space is limited, as information on national critical structures has the status of secret and is accordingly protected by national legislation since information security, as a component of national security is entrusted to specialized state institutions of national security, in particular the Ministry of Defense, the National Security Service, the Ministry of Internal Affairs.

However, there are quite important the approaches to information security adopted in the European Union which are currently not unified due to the geopolitical specifics of the EU and, accordingly, the experience of Central and Eastern Europe (including Bulgaria, Romania, Slovakia, Croatia, the Czech Republic) in the formation and development of a secure information society. Therefore, the study of the features of regulatory and legal support of information security of these countries in the context of the study of their national cyber strategies, as an immanent component of national security is the main purpose of this study.

Accordingly, based on the study, it can be noted that in their strategies, EU countries, in particular the Central-Eastern region of Bulgaria, Romania, Slovakia, Croatia, and the Czech Republic, are unanimous in their plans to integrate national cyber defense capabilities and expand resources to counter cyber attacks. Each of these countries also uses international cooperation to exchange information on cybersecurity and technical assistance. In addition, it is important that the national legislation of these countries is fully in force in this cooperation, although their specifics in the field of information security do not always correspond to the specifics of the regulatory framework of other countries and the European Union as a whole.

At the same time, the analysis of the legal and organizational foundations of the cybersecurity system of Eastern and Central Europe countries shows the dominant role of special services, including the military forces, in ensuring the cyber security of the state, due to the nature of cyber threats of today, which requires tools like powers, forms and methods inherent only in special namely counterintelligence agencies of the state.

Keywords: EU member states, information security, cybersecurity, information space, rule of law.