УДК 341
DOI https://doi.org/10.32849/2663-5313/2020.12.55

Святослав Кавин,
аспірант факультету міжнародних відносин
Львівського національного університету імені Івана Франка

НОРМАТИВНО-ПРАВОВІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В КРАЇНАХ БАЛТІЇ

Стаття присвячена вивченню особливостей нормативно-правового забезпечення інформаційної безпеки держав Європейського Союзу (зокрема, Естонії, Литви та Латвії) в контексті дослідження їхніх національних кіберстратегій. У статті представлено дослідження правових та інституційних механізмів забезпечення кібербезпеки країнами Балтії в умовах кризи сучасної системи міжнародної безпеки, спричиненої глобальною діджиталізацією суспільства. У дослідженні охарактеризовано кібербезпекові стратегії Естонії, Литви та Латвії, діяльність відповідних органів, які забезпечують інформаційну безпеку держав, а також спільні дії цих країн в контексті євроінтеграційних процесів щодо зміцнення захисту інформаційного простору. Також розглядаються міжнародно-правові аспекти різних підходів щодо забезпечення кібербезпеки.

Огляд національних стратегій кібербезпеки країн Балтії показав, що їхні кібербезпеки є комплексними і всеохоплюючими. Ці стратегії охоплюють економічні, соціальні, міжнародно-правові, правоохоронні та військові аспекти кібербезпеки. Разом із тим країни проводять різницю між внутрішніми і зовнішніми джерелами кіберзагроз у своїх стратегічних документах. У цьому контексті країни Балтії працюють над інтеграцією національних законодавств в уніфіковану міжнародно-правову платформу з метою зниження ризиків виникнення конфліктів унаслідок використання інформаційно-комунікаційних технологій. Кожна країна має свої стратегії кібербезпеки, і вони певною мірою мілітаризують питання захисту інформаційного простору. Ця тенденція піднімає кібербезпеку до рівня національної безпеки і фокусується на захисті державних ресурсів інформаційно-комунікаційних технологій. Важливим фактором є те, що держави активно сек'юритизують свій кіберпростір і приділяють першочергову увагу захисту критичної інфраструктури як ключовій умові національної безпеки. Власне, таке ставлення диктує силовий підхід до управління кібербезпекою як найбільш ефективний. Відповідно, відповідальність за нейтралізацію кіберзагроз та стабільність в інформаційному просторі покладається на силові структури.

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

Постановка проблеми. Глобалізація інформаційного простору, а відповідно, тотальна діджиталізація суспільства призвела до появи якісно нових видів загроз, зокрема: інформаційного тероризму, кібератак, кіберзлочинності та асиметричних воєн. Об'єктами цих загроз стають критично важливі інфраструктури, а відповідно, є серйозна загроза національній безпеці держави. Оскільки інформаційне суспільство, чи кібер-суспільство, не має кордонів, то вирішення питань безпечності та стабільності інформаційного простору в правовому полі є надзвичайно складним. Оскільки безпека національних інтересів кожної держави забезпечується національними законодавствами і не існує уніфікованої міжнародної правової платформи щодо забезпечення інформаційної безпеки, зокрема кібербезпеки, то дослідження шляхів вирішення цих проблем набуває надзвичайної актуальності.

Деякі держави розглядають забезпечення кібербезпеки як цивільну або економічну задачу, хоча багато держав залучають до вирішення цього завдання спецслужби, зокрема, для здійснення політики забезпечення кібербезпеки. Водночас міжнародна співпраця стосовно уніфікованих підходів до боротьби з кіберзагрозами в інформаційному просторі має дещо обмежений характер, оскільки спецслужби насамперед захищають національну критичну інфраструктуру від кіберзагроз і діють у рамках національних інтересів.

Проблематику інформаційної безпеки у держава-членах ЄС, зокрема у сфері кіберзахисту, досліджували у своїх роботах вітчизняні і зарубіжні науковці: В. Бутримас, О. Звоздецька, А. Ковалев, А. Балашов, S. Dimitrova, S. Stoykov, Y. Kochev, K. Newmeyer, L. J. Janczewski, A. M. Colarik. L. Kovacs, T. Mattila. Проте комплексні дослі-

дження з метою вивчення та порівняння нормативно-правового забезпечення інформаційної безпеки держав-членів ЄС, зокрема, в контексті уніфікації їхнього законодавства у даній сфері поки що недостатньо висвітлені в науковій літературі. Вивчаючи національне законодавство держав ЄС у сфері забезпечення інформаційної безпеки та протидії кіберзагрозам, а також досліджуючи їхню практику в цьому напрямі, А. Ковалев і А. Балашов [15, с. 105-114], а також В. Панченко [16, с. 91-100] сформували свої зауваження, суть яких полягає в тому, що поки не існує єдиної уніфікованої системи в цьому напрямі – кожна з держав має свої правові механізми щодо врегулювання даного кола питань, і в кожної з них існує своя унікальна система захисту інформації.

Метою статті є вивчення особливостей нормативно-правового забезпечення інформаційної безпеки країн Балтії в контексті дослідження їхніх національних кіберстратегій в умовах кризи сучасної системи міжнародної безпеки, спричиненої глобальною діджиталізацією суспільства.

Виклад основного матеріалу. Майже всі держави враховують загрози та ризики у кіберпросторі у своїй політиці національної безпеки. Ця проблема досліджується досить активно [18], [19], але її актуальність не зменшується, оскільки технології розвиваються настільки швидкими темпами, що ані політики, ані юристи, ані економісти, навіть IT-фахівці просто не встигають за динамікою реальності. Застосування основ теорії безпеки дозволяє розглядати як цивільні, так і силові підходи до питань забезпечення кібербезпеки і сприйняття можливих загроз та їх джерел. Існують різні доктрини, що розглядають питання кібербезпеки. Парадигма національної безпеки відображає традиційну роль держави в забезпеченні безпеки кордонів країни і дотриманні верховенства права [20]. Кібербезпека нині визнається одним із найважливіших факторів державної військової та економічної безпеки, її необхідність обґрунтовується традиційними аргументами національної безпеки, що базуються на захисті держави [12].

Diego Acosta Arcarazo та 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. Поєднання нового Договору та Програми зробило безпеку та правосуддя ключовими сферами законодавчого розвитку в ЄС [17, с. 17]. Це зауважує і Raphael Bossong, який зазначає, що важливий елемент співробітництва в галузі безпеки між країнами Європейського Союзу (ЄС) – це інтенсивний обмін інформацією між органами безпеки, а наявні підходи до розвідувальної підтримки політики безпеки ЄС повинні бути поглиблені та краще контролюватися [22, с. 6].

Prof. Dr. Udo Helmbrecht зазначає, що забезпечення мережевих та інформаційних систем Європейського Союзу в правовому полі має важливе значення для підтримки інтернет-економіки на основі впровадження нових ініціатив щодо подальшого покращення кібер-стійкості та реагування на кіберзахист [27]. У цьому контексті Laszlo Kovacs [21, с. 16-24], а також Sevdalina Dimitrova [23, с. 54-58] визначають стратегію кібербезпеки як базовий документ, що відображає інтереси та правила безпеки роботи в кіберпросторі, а також встановлює основу для майбутнього законодавства та міжнародних стандартів щодо безпеки інформаційного простору від кіберзагроз.

У цьому контексті в країнах Європейського Союзу, що активно займаються реалізацією політики кібербезпки, є досить цікавий досвід країн Балтії, зокрема Естонії, Литви, Латвії.

Естонія. Найбільш розвиненою в області кіберзахисту і захищеною від кіберзагроз в інформаційному просторі серед країн Балтії є Естонія.

Естонська Республіка одна з перших у світі прийняла Національну стратегію кібербезпеки, яка чітко була вписана в рамки міжнародного права. А у 2014 р. був прийнятий новий документ «Стратегія кібербезпеки на 2014-2017 рр.» (Cyber Security Strategy, 2014) [3]. Як зазначає Звоздецька, стратегічними цілями Естонії у сфері кібербезпеки, які викладені в Стратегії, є створення багаторівневої системи без пекових заходів, а також правове регулювання питань кібербезпеки. У багаторівневій системі безпекових заходів пріоритетне значення надається захисту критичної інформаційної інфраструктури. А стратегічне планування забезпечує згуртованість усієї архітектури кібербезпеки, а також полегшує використання інформаційно-комунікаційних технологій і розробку «розумних рішень» [14, с. 20-34].

До 2011 р. координацію політики держави в області кібербезпеки забезпечувало Міністерство оборони Естонії, а з 2011 р. відповідальність за координацію політики в області кібербезпеки Естонії перейшла від Міністерства оборони до Міністерства

з економічних питань та комунікацій. Міністерство оборони є координаційним органом для кібернетичної оборони в загальній системі національної оборони. Відповідно, розробка і впровадження політики інформаційної безпеки належить до компетенції саме Міністерства з економічних питань та комунікацій, зокрема до його структурних підрозділів, таких як Департамент державних інформаційних систем та Естонський центр інформатики [7]. У червні 2011 р. Естонський центр інформатики був трансформований в Управління інформаційних систем Естонії (Estonian Information Systems Autority (EISA)). В Управління інформаційних систем Естонії входять ряд структурних підрозділів, які комплексно забезпечують кібербезпеку держави, зокрема: Департамент із захисту критичних інформаційних інфраструктур (Critical Information Infrastructure Protection (CIIP)), Центр обміну документами (About document exchange centre (DEC)), Інфраструктура відкритих ключів (Public Key Infrastructure (PKI)), IT-інфраструктура (IT-infrastructure). Інфраструктура відкритих ключів забезпечує безпеку цифрову аутентифікацію і цифрові підписи. IT-інфраструктура забезпечує доступність основних інформаційних послуг держави навіть у разі форс-мажорних обставин [9].

Разом із тим в Естонії, у Комітеті з питань безпеки Естонського уряду, створено Раду з кібербезпеки Естонії, яка, будучи міжвідомчим органом, надає підтримку у міжвідомчій співпраці на стратегічному рівні, а також здійснює нагляд за реалізацією цілей стратегії кібербезпеки країни.

У 2006 р. в Естонії створена група швидкого реагування (CERT Estonia). Ця структура відповідає за управління безпековими інцидентами у комп'ютерних мережах. А у травні 2008 р. у Брюсселі (Швейцарія) був підписаний меморандум про створення в Естонії, у м. Таллінн, Центру передових технологій з кібербезпеки НАТО. Відповідно, з 2008 р. у складі сил оборони Естонії створений і діє Центр передового досвіду НАТО з кіберзахисту – Міжнародна військова організація, яка зосереджує свої зусилля на розширенні можливостей кібернетичної оборони НАТО і країн-партнерів. НАТО офіційно визнало кіберпростір операційним середовищем і таким чином прирівняло існуючі в ньому загрози до військових загроз. Також у 2017 р. в Таллінні був створений Об'єднаний центр передових технологій з кіберзахисту НАТО (NATO Cooperative Cyber Derence Centre of Excellence), який є флагманом європейської кібербезпеки. Основне завдання Центру – тренування фахівців з різних країн, які забезпечують безпеку в національному кіберпросторі [1].

Латвія. Основоположними документами, що визначають політику Латвії у сфері кібербезпеки, є Концепція національної безпеки 2011 р. та Стратегія кібербепеки Латвії 2014-2018 рр. (Cyber Security Strategy of Latvia 2014-2018) [4].

Стратегія кібербезпеки Латвії на 2014-2018 роки була першим документом щодо політики в галузі кібербезпеки, і деякі її заходи, наприклад моніторинг інфраструктури ІКТ, поширюються на період до 2022 року.

Основне завдання Стратегії – це розробка законодавчої бази для кібербезпеки та систем безпеки ІКТ у всіх секторах. Вона описує контекст кібербезпеки Латвії, визначає майбутні виклики та пріоритети національної політики кібербезпеки.

Політика кібербезпеки спрямована на зміцнення та вдосконалення можливостей кібербезпеки шляхом підвищення стійкості проти кібератак та підвищення обізнаності громадськості про загрози в кіберпросторі. Як зауважує Ковальов, для досягнення своєї мети політика пропонує дії у п'яти сферах: посилення кібербезпеки та керовані ризики цифрової безпеки; стійкість систем ІКТ; кращий універсальний доступ до стратегічних систем та послуг ІКТ; поінформованість громадськості, освіта та дослідження; міжнародне співробітництво; верховенство закону в кіберпросторі та запобігання кіберзлочинності [15, с. 105-114].

У Стратегії кібербезпеки розглядаються загрози, пов'язані з безпекою інформаційно-комунікаційних технологій в кіберпросторі, і дається прогноз щодо ризиків кібернебезпеки на майбутнє, а в Законі Латвії про безпеку інформаційних технологій (Law On the Security of Information Technologies) визначаються основні вимоги щодо безпеки для державних і муніципальних установ [10]. Ці два документа віддзеркалюють комплексний підхід до захисту безпеки в кіберпросторі і національної безпеки Латвії в цілому. У рамках цієї політики визначені такі напрями діяльності: управління кібербезпекою, правопорядок у кіберпросторі і зниження рівня кіберзлочинності, дослідницька робота в цій сфері, а також міжнародна співпраця. Міністерство оборони Республіки координує участь Латвії у формуванні міжнародної політики у сфері кібербезпеки.

Національну політику у сфері кібербезпеки забезпечують:

1. Міністерство оборони (МО) – координує розробку і впровадження інформацій-

них технологій, політику безпеки і захисту інформаційних систем, а також забезпечує міжнародне співробітництво.

2. Міністерство внутрішніх справ (МВС), Державна поліція (ДП) і Поліція безпеки (SeP) – здійснюють політику у сфері боротьби зі злочинністю, охорони правопорядку, забезпечення безпеки, а також координує врегулювання кризових ситуацій.

3. Латвійський Центр з протидії кіберзагрозам (CERT.LV) – здійснює моніторинг і аналіз подій в кіберпросторі, реагує на кіберінциденти, здійснює їх координацію та профілактику, проводить дослідження. CERT відповідає за безпеку у всьому латвійському електронному інформаційному просторі.

Перша Команда реагування на кіберінциденти (LATNET CERT) була створена ще у 2006 р., і на її основі у 2011 р. було створено Латвійський Центр з протидії кіберзагрозам (CERT.LV), що працює при Міністерстві оборони Латвійської Республіки і регулюється Законом «Про безпеку інформаційних технологій» [2].

4. Центр забезпечення безпечного Інтернету в Латвії (Operation of the Safer Internet Centr of Latvia NetSafe) – інформує суспільство про можливі ризики і загрози онлайн, сприяє використанню безпечного Інтернет-контенту.

5. Національні збройні сили і кібернетичної оборони (Unit National Armed Forces (NAF) and Cyber Defence Unit (CDU)) – надають підтримку в кризових ситуаціях.

Кібербезпека є частиною всеосяжної національної системи оборони. Враховуючи потенційний національний та соціальний вплив кібератак, кібербезпека стає дедалі важливішою у всебічній національній обороні.

У 2014 р. в Норфолку (США) був підписаний меморандум про створення в Ризі міжнародного Центру стратегічних комунікацій. Центр працює як центральний осередок для обговорення та експертизи різних дисциплін зі сфери стратегічних комунікацій: публічної дипломатії, військових зв'язків з громадськістю, інформаційних і психологічних операцій. А 20 серпня 2015 р. в Ризі відкрився новий офіс Центру стратегічних комунікацій НАТО (Stratcom). Завданнями центру є: розроблення програм для сприяння розвитку та гармонізації доктрини стратегічних комунікацій; проведення дослідження та експериментів з метою пошуку практичних рішень для розв'язання існуючих проблем; «вивчення уроків» застосування стратегічних комунікацій під час військових операцій. Нині Центр визначає стратегічні комунікації як «скоординоване і належне використання комунікативної діяльності і можливостей НАТО з метою підтримки політики, операцій і діяльності Альянсу, а також в цілях просування цілей НАТО. Цією діяльністю та можливостями є: публічна дипломатія, військові зв'язки із громадськістю, операції та психологічні операції» [6].

Литва. За Глобальним індексом кібербезпеки, складеним Міжнародним союзом електрозв'язку, Литва займає 57-е місце. Загалом, цей індекс відображає рівень кіберзахищеності держав і зусилля, які докладає конкретна країна для поліпшення цього показника.

Документи, що забезпечують кібербезпеку Литовської Республіки, – це: «Програма розвитку електронної інформаційної безпеки (кібербезпека) на 2011-2019 рр.» (Resolution no 796 of 29 June 2011. On the Approval of The Programme for the Development of Electronic Information Security (Cyber-Security) for 2011–2019), яку Уряд Литви схвалив з метою забезпечення безпеки кіберпростору держави і яка була затверджена 29 червня 2011 р. [11], та Закон «Про Кібербезпеку» (National legislation Cybersecurity Act (2014)) прийнятий у 2014 р., за яким кібербезпека визначається як сукупність правових, організаційних і технічних заходів для запобігання, виявлення, аналізу і реагування на кіберінциденти, а також відновлення нормального функціонування систем управління електронних мереж зв'язку, інформаційних систем або промислових процесів у разі кібератак [8].

Як зауважує Звоздецька, мета Програми полягає у визначенні цілей і завдань для розвитку електронної інформації з метою забезпечення конфіденційності, цілісності та доступності електронної інформації та послуг, що надаються в кіберпросторі, охорони електронних комунікаційних мереж, інформаційних систем і критично важливих інформаційних інфраструктур від інцидентів і кібератак. Цілями Програми були заявлені зміцнення безпеки державних інформаційних ресурсів, а також забезпечення ефективного функціонування критичної інформаційної інфраструктури [14, с. 20-34].

Відповідно до чинного законодавства Литовської Республіки, Міністерству оборони надано право координувати національну політику з кібербезпеки, передбачається також діяльність Національного центру кібербезпеки, Консультативної ради з кібербезпеки при Міністерстві оборони, а також створення та діяльність сил швидкого реагування на кіберзагрози (CERT).

CERT-LT є національною командою литовського Computer Emergency Response,

завданням якого є забезпечення безпеки в інформаційному суспільстві шляхом запобігання, моніторингу та вирішення інцидентів інформаційної безпеки, поширення інформації про загрози інформаційної безпеки. Метою CERT-LT є надання можливості для вирішення питаньимережевої та інформаційної безпеки, моніторинг кіберінцидентів та їх профілактика; координація дій інтернет-провайдерів, телекомунікаційних мереж операторів і CERT груп в Литві під час відповіді на мережеві та інформаційні інциденти; дослідження вразливості мереж та інформаційних систем; поширення інформації про загрози для мережевої та інформаційної безпеки; сприяння створенню нових груп CERT [5].

У червні 2018 р. Сейм Литви прийняв зміни до закону про кібербезпеку. Відповідно до поправок, підготовлених Міноборони Литви, Уряд держави прийняв Національну стратегію захисту від кіберзагроз в контексті розвитку міжнародного співробітництва та управління ризиками на рівні Європейського союзу.

Разом із тим у Вільнюсі 14 січня 2011 р. під керівництвом литовського Міністерства закордонних справ був відкритий Центр передового досвіду НАТО з питань енергетичної безпеки (ENSEC COE).

Ковальов зазначає, що місія Центру передового досвіду НАТО з питань енергетичної безпеки полягає в тому, щоб допомогти органам НАТО, країнам і партнерам та іншим цивільним і військовим органам шляхом надання експертних рекомендацій з усіх аспектів енергетичної безпеки. Центр реалізує проекти у сферах безпеки з дотриманням трьох аспектів енергетичної безпеки відповідно до Уельського Саміту НАТО: підвищення рівня поінформованості з питань розвитку енергетики з наслідками для безпеки, підтримка захисту критично важливої енергетичної інфраструктури та підвищення ефективності використання енергії в збройних силах. Ці напрями забезпечуються за рахунок трьох підрозділів Центру: стратегічного аналізу і досліджень; освіти, підготовки і навчання; доктрини та концепції розвитку [15, с. 105-114].

Висновки

Дослідження національних стратегій кібербезпеки в країнах Балтії показало, що їхні кібербезпеки є комплексними і всеохоплюючими. Ці стратегії охоплюють економічні, соціальні, міжнародно-правові, правоохоронні та військові аспекти кібербезпеки. У рамках співпраці по лінії ОБСЕ та НАТО країни Балтії працюють над інтеграцією національних законодавств в уніфіковану міжнародно-правову платформу з метою зниження ризиків виникнення конфліктів унаслідок використання інформаційно-комунікаційних технологій. Вони визнають взаємозв'язок між сферою кібер- і національної безпеки і усвідомлюють, що проблеми кібербезпеки, такі як руйнування системи інформаційно-комунікаційних технологій чи критичної інфраструктури, можуть завдати шкоди національній безпеці і функціонуванню економіки держави.

Усі три держави активно сек'юритизують свій кіберпростір і приділяти першочергову увагу захисту критичної інфраструктури як ключовій умові національної безпеки. Власне таке відношення диктує силовий підхід до управління кібербезпекою як найбільш ефективний. Зосередження уваги головним чином на внутрішніх загрозах означає, що основним об'єктом безпеки виступає економічна сфера.

Важливо зауважити, що у своїх стратегічних документах країни проводять різницю між внутрішніми і зовнішніми джерелами кіберзагроз. Кожна країна має свою стратегію кібербезпеки, і вони певною мірою мілітаризують питання кіберзахисту. Ця тенденція піднімає кібербезпеку до рівня національної безпеки і, власне, фокусується на захисті державних ресурсів інформаційно-комунікаційних технологій. Відповідно, основна відповідальність за нейтралізацію кіберзагроз покладається на силові структури.

Список використаних джерел:

1. About CERT Estonia. URL: https://www.ria.ee/en/cert-estonia.html (дата звернення: 10.10.2020).
2. CERT.LV. URL: www.cert.lv/lv/par-mums (дата звернення: 10.10.2020).
3. Cyber Security Strategy (2014). URL: https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf (дата звернення: 10.10.2020).
4. Cyber Security Strategy of Latvia 2014-2018. URL: www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss (дата звернення: 10.10.2020).
5. CERT-LT URL: https://www.cert.lt/en/ (дата звернення: 10.10.2020).
6. NATO Strategic Communications Centre of Excellence Riga, Latvia. URL: http://www.stratcomcoe.org/ (дата звернення: 12.10.2020).
7. National Security Concept of Estonia (2010). URL: https://www.kaitseministeerium.ee//sites/default/files/elfinder/article_files/julgeolekupoliitika_alused_2010.pdf (дата звернення: 10.10.2020).
8. National legislation Cybersecurity Act (2014). URL: https://ccdcoe.org/sites/default/

files/strategy/LTU_CSAct_lt.pdf (дата звернення: 12.10.2020).

9. The Estonian Informatics Centre became the Estonian Information System's Authority. 16.06.2011. URL: https://www.ria.ee/en/the-estonian-informatics-centre-became-theestonian-information-systems-authority.html (дата звернення: 10.11.2020).

10. Law On the Security of Information Technologies. URL: http://www.dvi.gov.lv/en/legal-acts/law-on-the-security-of -information-technologies/ (дата звернення: 10.10.2020).

11. Resolution no 796 of 29 June 2011. On the Approval of The Programme for the Development of Electronic Information Security (Cyber-Security) for 2011–2019. URL: http://www.ird.lt/doc/teises_aktai_en/EIS(KS)PP_796_201-06-29_EN_PATAIS.pdf (дата звернення: 10.10.2020).

12. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность ка основной фактор национальной и международной безопасности XXI века (ч. 1). *Вопросы безопасности*.

13. Бутримас Витаутас. Балтийское сотрудничество в области кибербезопасности. *Per Concordiam*. 2016. № 2. Том 7. С. 19-23.

14. Звоздецька О. Кібербезпека країн Балтії: сучасні виклики та загрози. *Медіафорум : аналітика, прогнози, інформаційний менеджмент: збірка наукових праць*. Чернівці: Чернівецький національний університет, 2017. Том 5. С. 20-34.

15. Ковалев А.А., Балашов А.И. Международно-правовые аспекты политики кибербезопасности некоторых европейских стран бывшего советского блока. *Вестник Поволжского института управления*. 2018. № 5 (18). С. 105–114.

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

17. 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.

18. Janczewski L.J., Colarik A.M. Cyber warfare and cyber terrorism. N.Y., 2008.

19. Cyberterrorism / ed. by Alan O'Day. Burlington: Aldershot Hants, 2004.

20. Newmeyer K.P. Elements of national cybersecurity strategy for developing nations. *National Cybersecurity Institute Journal*. 2015. № 1(3). P. 9–19.

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

22. 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.

23. 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.

24. 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.

Sviatoslav Kavyn. Regulatory mechanisms for guaranteeing cybersecurity in the Baltic States

An article is devoted to the study of the peculiarities of the regulatory and legal support of information security of the European Union (in particular Estonia, Lithuania and Latvia) in the context of the study of their national cyberstrategies. The articles present a study of legal and institutional mechanisms for cybersecurity in the Baltic States in the crisis of the modern international security system with a view to the global digitalization of society. There is described cybersecurity strategy of Estonia, Lithuania and Latvia, the activities of the relevant bodies, which ensure the information security of the state, including and cybersecurity, as well as joint actions of these countries in the context of European integration processes to strengthen the protection of the information space. International legal aspects of different approaches to cybersecurity.

A review of the national cybersecurity strategies of the Baltic States has shown that their cybersecurity is comprehensive and inclusive. These strategies cover the economic, social, international law, law enforcement and military aspects of cybersecurity. At the same time, countries provoke the difference between internal and external sources of cyber threats in their strategic documents. In this context, the Baltic States are working to integrate national legislation into a unified international legal platform to help reduce the risk of conflicts in national legislation using information and communication technologies. Each country has its own cybersecurity strategies and they privately militarize the protection of the information space. This trend connects cybersecurity to the level of national security and focuses on the protection of public information and communication technology resources. An important factor is that the state is actively securitizing cyberspace and we is prioritizing the protection of critical infrastructure as a key condition of national security. In fact, such a recovery dictates a forceful approach to cybersecurity management as the most effective. Responsibility for neutralizing cyber threats and stability in the information space is given to law enforcement agencies.

Key words: EU, information security, cybersecurity, information space, rule of law.