УДК 341
DOI https://doi.org/10.32837/apdp.v0i87.2797

С. Я. Кавин

ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ДЕРЖАВАХ – ЧЛЕНАХ ЄВРОПЕЙСЬКОГО СОЮЗУ

Постановка проблеми. Найважливішим результатом формування інформаційного суспільства стала поява глобального інформаційного простору, а водночас сформувались нові форми конфліктів, які значно інтенсивніші та масштабніші, отже, становлять серйозну загрозу національній безпеці держав. Досвід країн Європейського Союзу (далі – ЄС), зокрема й країн Центрально-Східної Європи, показує, що належний захист від викликів інформаційних воєн, зокрема різних видів кіберзагроз (кібератаки, кібершпигунство), може бути реалізований лише за допомогою ефективної та надійної системи інформаційної безпеки на основі ефективної стратегії кібербезпеки та відповідних механізмів управління, якими виступають державні інститути національної безпеки.

Сьогодні країни Центрально-Східної Європи сформували національні мережі інформаційної безпеки, які здатні швидко накопичити сили та засоби державних органів для протидії, зокрема кіберзагрозам, тим самим гарантувати національну безпеку своїх країн. Але оскільки обов'язок щодо гарантування інформаційної безпеки як складової частини національної безпеки держав покладено на державні спеціалізовані інституції національної безпеки (міністерства оборони, служби національної безпеки, міністерства внутрішніх справ), то міжнародна співпраця стосовно уніфікованих підходів до боротьби з кіберзагрозами в інформаційному просторі має деякою мірою обмежений характер, оскільки інформація щодо національних критичних структур має статус секретної й охороняється відповідними національними законами.

Окрім того, хоча кожна із країн Центрально-Східної Європи має досить міцну правову базу в цій галузі, обмеження інформаційного доступу щодо функціональних підходів національних спеціалізованих інституцій у боротьбі з кіберзагрозами являють собою проблеми, які полягають у невідповідності законодавств у підходах до вирішення окремих питань інформаційної безпеки, що значно знижує ефективність правового регулювання в цій галузі.

Водночас підходи до інформаційної безпеки, поширені в Європейському Союзі, нині не є уніфікованими через геополітичну специфіку держав ЄС, отже, досвід країн Центрально-Східної Європи у процесі становлення та розвитку інформаційного суспільства є досить важливим. Тому дослідження, оцінка та реалізація позитивного досвіду кожної із цих країн важливі під час побудови системи інформаційної безпеки Європейського Союзу в контексті надійного захисту від кіберзагроз.

Результати аналізу наукових публікацій. Проблематику інформаційної безпеки у країнах Центрально-Східної Європи, зокрема в області кіберзахисту, досліджували у своїх працях вітчизняні та закордонні науковці: Т. Ткачук, О. Климчук,

Н. Ткачук, А. Ковалев, А. Балашов, Sevdalina Dimitrova, Stoyko Stoykov, Yosif Kochev, Marek Gorka, Tam s Szadeczky, L szl Kovacs, Turo Mattila. Проте проведення комплексного дослідження з метою вивчення та порівняння нормативно-правового забезпечення інформаційної безпеки ЄС, зокрема в області кіберзахисту, у контексті можливої кореляції законодавств країн Центрально-Східної Європи у сфері кіберзахисту з метою оптимізації законодавчої бази ЄС поки що висвітлені в науковій літературі недостатньо.

Сучасні реалії політики національної безпеки країн Центрально-Східної Європи потребують комплексних досліджень у контексті забезпечення національних інтересів, розроблення ефективних механізмів захисту інформаційного простору, дослідження політичних та правових механізмів побудови інформаційної безпеки.

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

Презентація основного матеріалу. У процесі проведення аналізу національних законодавств держав ЄС у сфері гарантування інформаційної безпеки та протидії кіберзагрозам, а також дослідження їхньої практики в цьому напрямі А. Ковалев і А. Балашов у роботі «Международно-правовые аспекты политики кибербезопасности некоторых европейских стран бывшего советского блока» [5, с. 105–114], а також В. Панченко у праці «Зарубіжний досвід формування систем захисту критичної інфраструктури від кіберзагроз» [7, с. 91–100] зауважують, що поки не існує єдиної уніфікованої системи в цьому напрямі, кожна з держав має свої правові механізми щодо врегулювання цих питань, у кожної з них існує своя унікальна система захисту інформації.

Diego Acosta Arcarazo і Cian C. Murphy зазначають, що набрання чинності Лісабонським договором надало ЄС нові повноваження в галузі права міжнародної безпеки, водночас 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 [10, с. 17]. На цьому робить акцент і Raphael Bossong, який зазначає, що важливий елемент співробітництво в галузі безпеки між країнами Європейського Союзу – інтенсивний обмін інформацією між органами безпеки. Хоча в цій чутливій області не варто очікувати якихось особливих кроків на шляху інтеграції. Однак наявні підходи до розвідувальної підтримки політики безпеки ЄС мають бути поглиблені та краще контролюватися [14, с. 6].

Професор Udo Helmbrecht зазначає, що забезпечення мережевих та інформаційних систем Європейського Союзу у правовому полі має велике значення для підтримки інтернет-економіки на основі впровадження нових ініціатив щодо подальшого покращення кіберстійкості [17]. У цьому контексті Laszlo Kovacs у своїй роботі "Cyber Security Policy and Strategy in the European Union and NATO" [12, с. 16–24], а також Sevdalina Dimitrova, Stoyko Stoykov і Yosif Kochev у праці "National

Cybersecurity Strategies in Member States of the European Union" [15, с. 54–58] визначають стратегію кібербезпеки як базовий документ, створений в урядовому контексті, що відображає інтереси та правила безпеки роботи в кіберпросторі. Крім того, встановлює основу для майбутнього законодавства, політики / стандартів, керівних принципів та інших рекомендацій щодо безпеки та кібербезпеки.

У цьому ж контексті представляє інтерес досвід деяких країн Східної Європи, зокрема Польщі й Угорщини.

Польща. Кібербезпека є частиною системи національної безпеки Польщі. Уперше питання кібербезпеки країни було порушено у 2007 р., зокрема у Стратегії національної безпеки. У ній відзначався прямий зв'язок між кібербезпекою і здатністю держави функціонувати належним чином. У 2014 р. Стратегія була оновлена, у ній детально були висвітленні питання, пов'язані із захистом кіберпростору в Польщі.

О. Климчук і Н. Ткачук у роботі «Роль і місце спецслужб та правоохоронних органів провідних країн світу в національних системах кібербезпеки» [6, с. 75–83] зазначають, що основні функціональні повноваження в гарантуванні кібернетичної безпеки Польщі покладено на Агентство внутрішньої безпеки (ABW). У 2013 р. за участю даного органу розроблено Стратегію кібербезпеки Польщі (National Security Strategy of the Republic of Poland) [4] та створено при Міністерстві національної оборони Центр криптології, на який покладено завдання із захисту інформації, кібероборони та проведення наступальних кібероперацій. ABW також сформувало урядову команду реагування на комп'ютерні інциденти (CERT), головним завданням якої є забезпечення і розвиток можливостей органів державного управління щодо захисту від кіберзагроз. Під керівництвом ABW у 2015 р. розроблено Доктрину кібербезпеки Польщі (Cybersecurity doctrine of the Republic of Poland) [1], яка оперує ключовими поняттями теорії безпеки на кшталт «загроз», «викликів», «ризиків» тощо. У Доктрині визначені цілі щодо підвищення національної безпеки в області кіберпростору. У 2015 р. в Польщі розпочато роботу над Доктриною інформаційної безпеки.

У своїй роботі "Cybersecurity in Central Eastern Europe: from identifying risks to countering threats" Agnija Tumkevič [9, с. 73–88] зазначає, що Доктрина інформаційної безпеки Польщі розглядається як виконавчий документ до Стратегії національної безпеки. Іншою особливістю правового регулювання інформаційної безпеки в Польщі є безпосередній вплив на політику держави в інформаційній сфері. У цьому документі підкреслюється, що будь-які польські положення повинні бути сумісні зі стратегіями союзних держав та міжнародних організацій, як-от ЄС та НАТО.

Як зазначає Marek Gorka у своїй праці "The Cybersecurity Strategy of the Visegrad Group Coutries" [13, с. 75–98], основна мета стратегії – гарантування безпеки Польщі в кіберпросторі. Стратегія окреслює деякі виклики, з якими Польща продовжує стикатися, і найважливіші завдання з кібербезпеки країни, що включає розроблення системного підходу, який матиме правовий, організаційний і технічний аспекти. У документі зазначено, що розширення кібербезпеки створює потенціал для значного наукового співробітництва. Отже, виникає потреба створити систему підтримки досліджень і розробок із кібербезпеки й освіти. Ще одним клю-

човим моментом є важливість постійного розвитку збройних сил. У даному документі звертається особлива увага на розвідувальні та контррозвідувальні служби.

Як видно, Польща робить акцент на розширення повноважень та можливостей спецслужб у кіберпросторі, оскільки це дозволить їм нейтралізувати діяльність зовнішньої розвідки. У цьому контексті політика кібербезпеки повинна запровадити безпечну систему нагляду, тобто незалежну комунікаційну мережу для управління національною безпекою (це можна зробити, наприклад, у межах урядової мережі зв'язку). Важливо також забезпечити національний контроль за системами ІКТ.

Угорщина. Правове забезпечення інформаційної сфери Угорщини, зокрема й кібербезпеки, втілено в Законі «Про електронну інформаційну безпеку державних та муніципальних органів» (2013 р.) та Стратегії національної безпеки Угорщини, затвердженої у 2012 р. (Hungary's National Security Strategy) [2]. Стратегія національної безпеки, зокрема, передбачає, що держава має бути готова управляти ризиками й загрозами, пов'язаними з національною безпекою, обороною, боротьбою проти злочинності, а також запобігати нештатним ситуаціям у кіберпросторі. Водночас основним завданням визнається систематичне визначення пріоритетів у сфері потенційних загроз і ризиків у кіберпросторі, а також підвищення поінформованості суспільства щодо них. Щодо міжнародного співробітництва, то основна мета – це розширити роль Угорщини в ініціативах і співробітництві в кібернетичному захисті ЄС та НАТО, а також у проєктах співробітництва в галузі кібербезпеки ООН і ОБСЄ.

Національна стратегія кібербезпеки Угорщини ухвалена у 2013 р. (National Cyber Security Strategy of Hungary) [3]. У ній чітко прописано, що захист суверенітету країни в кіберпросторі є національним інтересом. Уряд Угорщини вважає вкрай важливим, щоб кібербезпека стала питанням колективної оборони відповідно до ст. 5 основоположного договору НАТО. Це важливий крок на шляху міжнародно-правового гарантування кібербезпеки. Варто зазначити, що кіберзагрози також є пріоритетними у Стратегії національної безпеки Угорщини, ухваленої у 2012 р.

Угорська стратегія кібербезпеки в основному зосереджена на здійсненні національних інтересів у контексті самої держави. У ній встановлені цілі політики безпеки, зокрема, гарантування економічної безпеки, адаптація до технологічних інновацій та забезпечення міжнародного співробітництва в галузі кібербезпеки повинні бути сумісними з державними інтересами Угорщини, але водночас у контексті глобального кіберпростору. У документі також перелічені інструменти для підтримання та підвищення рівня кібербезпеки. Зокрема, безпечне використання кіберпростору залежить від чіткої й ефективної координації діяльності уряду.

У своїй роботі «Забезпечення інформаційної безпеки у країнах центральної Європи» Тарас Ткачук [8, с. 104–110] зазначає, що в документі визначено дві конкретні цілі для кіберстратегії, а саме: управляти загрозами та ризиками, що виникають у кіберпросторі, а також посилити координацію та ресурси уряду. Окрім того, також є посилання на такі цінності, як свобода, безпека та верховенство закону, а також необхідність міжнародного і європейського співробітництва. Угорська стратегія висвітлює міжнародні матеріали, які послужили покажчиками національного документа.

Також Стратегія відповідає рекомендаціям Європейського парламенту для держав ЄС, які включені до рішення № 2012/2096 (INI) про кібербезпеку й оборону, ухваленого 22 листопада 2012 р.; спільного повідомлення, опублікованого Європейською комісією та Верховним представником спільної зовнішньої політики та політики безпеки Європейського Союзу 7 лютого 2013 р. під назвою «Стратегія кібербезпеки Європейського Союзу: відкритість, безпечність та безпечний кіберпростір». Крім того, Стратегія відповідає Стратегічній концепції НАТО, ухваленої в листопаді 2010 р., Політиці кібербезпеки Організації, ухваленій у червні 2011 р., та її плану реалізації, а також принципам та цілям кіберзахисту, викладеним у документах самітів НАТО, які відбулися 19–20 листопада 2010 р. в Лісабоні та 20–21 травня 2012 р. в Чикаго.

Досить цікавий той факт, що Стратегія Угорщини запроваджує та визначає поняття «угорський кіберпростір», що включає як електронні інформаційні системи, розташовані на державній території, так і соціальні та фінансові процеси, що відбуваються всередині і через кіберпростір. Що стосується стандартів безпеки міжнародних організацій, кіберстратегія звертається до поняття оборони, що базується на загальному принципі оборони відповідно до ст. 5 Статуту НАТО. Отже, Угорщина визнає співпрацю з НАТО ключовою для кібербезпеки.

Стратегія також відзначає динамічний шлях розвитку нових технологій, як-от хмарні обчислення та мобільний інтернет, що призводить до постійної появи нових загроз безпеці. Також визначено кібербезпеку як постійний і запланований процес мінімізації кіберзагроз за допомогою політичних, правових, економічних, освітніх і технічних засобів. Варто зауважити, що у Стратегії також акцентовано наукові розробки в області кібербезпеки, системні взаємини з науковою спільнотою.

Також у національній кіберстратегії виділено потенційні загрози для держави, які можуть виникнути внаслідок витоку інформації. У цьому контексті звертається увага на безпеку ключової інфраструктури кіберпростору. У документі зосереджено увагу на співпраці й ефективному обміні інформацією із залученням наукових експертів різних профілів. Окрім того, у Стратегії також підкреслює важливість спеціалізованих інститутів політики безпеки.

Водночас, як зауважує Marek Gorka [13, с. 75–98], необхідно зазначити, що організації, відповідальні за політику кібербезпеки, чітко не вказані в документі, і на практиці це положення може спричинити багато суперечливих дій. І все ж, як зазначає у своїй праці “Cybersecurity in Central Eastern Europe: from identifying risks to countering threats” Agnija Tumkevi [9, с. 73–88], основним органом, відповідальним за координацію та реалізацію кіберзахисту в Угорщині, є Національна рада координації кібербезпеки. Окрім того, є додаткові установи, відповідальні за аспекти кібербезпеки, зокрема це: Національне управління кібербезпеки, яке створене при Міністерстві національного розвитку, Управління національної безпеки, яке створене при Міністерстві державного управління та юстиції, а також CERT. У своїй роботі “Information Security Law and Strategy in Hungary” Tamás Szadeczky [16, с. 281–289] зауважує, що Національне управління кібербезпеки, як спеціалізований орган, займається криміналістичним аналізом журналів та тестуванням кіберврразливості, а урядова команда реагування на надзвичайні ситуації у сфері комп’ютерних ситуацій (GovCERT) була передана різним органам влади.

Висновки. Проблема гарантування інформаційної безпеки через поширення кіберзагроз різного типу стає питанням державної безпеки. Кіберзагрози можуть спричинити зниження ефективності установ, які значною мірою покладаються на інформаційні технології, зокрема й критичної інфраструктури. Це особливо важливо для економіки Центральної та Східної Європи, яка все ще перебуває у процесі модернізації і є набагато більш чутливою до кіберінцидентів різного типу. Тому співпраця в рамках політики безпеки є особливо важливою для країн у цьому регіоні.

У своїх стратегіях держави одностайні щодо своїх планів у намаганні розширити 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. Нинішня політика кібербезпеки також відповідає їхнім обов'язкам як учасників НАТО та ЄС. Вони є частиною Європейської платформи безпеки в кіберпросторі і формують свою політику безпеки на співпраці з Європолом, Європейським центром кіберзлочинності (EC3) та Європейським агентством з питань мережевої та інформаційної безпеки (ENISA). Окрім того, важливо те, щоб під час цієї співпраці повною мірою діяло законодавство цих країн, регулювало нормативно-правові аспекти інформаційної безпеки, специфіка яких не завжди співвідноситься з особливостями нормативно-правової бази інших країн та ЄС загалом. Цей принцип є одним із найважливіших завдань у сфері застосування інформаційної безпеки.

Аналіз нормативно-правових і організаційних основ системи кібербезпеки країн Східної та Центральної Європи свідчить про домінантну роль спецслужб, зокрема військових, у гарантуванні кібернетичної безпеки держави, що пов'язано з характером кібернетичних загроз сьогодення, протидія яким потребує інструментарію (повноваження, форми, методи), притаманного суто спеціальним, а саме контррозвідувальним, органам держави. Вказані вище органи наділяються функціями здійснення міжвідомчої координації суб'єктів кібербезпеки держави. У їхніх структурах із метою впровадження ефективного й оперативного механізму протидії кіберзагрозам створюються національні центри кібербезпеки, до складу яких також входять і команди швидкого реагування на кіберінциденти (CERT).

Література

1. Cybersecurity doctrine of the Republic of Poland. URL: http://en.bbn.gov.pl/ftp/dok/01/DCB.pdf.

2. Hungary's National Security Strategy (2012). URL: https://www.ecfr.eu/page/-/Hongrie_-_2012_-_National_Security_Strategy.pdf.

3. National Cyber Security Strategy of Hungary (2013). URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf.

4. National Security Strategy of the Republic of Poland (as amended in 2014). URL: https://www.files.ethz.ch/isn/156796/Poland-2007-eng.pdf.

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

6. Климчук О., Ткачук Н. 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.

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

8. Ткачук Т. Забезпечення інформаційної безпеки у країнах центральної Європи. *Юридичний науковий електронний журнал.* 2017. № 5. С. 104–110.

9. Tumkevič Agnija. Cybersecurity in Central Eastern Europe: from identifying risks to countering threats. *Baltic journal of political science.* 2016. December 2016. № 5. P. 73–88.

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

11. Dimitrov N., Valentin Najdenov. National Security in Bulgaria – is it really a system? *Security & Future :* International Scientific Journal. 2019. P. 83–86.

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

13. Gorka Marek. The Cybersecurity Strategy of the Visegrad Group Countries. *Politics in Central Europe.* 2018. № 14 (2). P. 75–98.

14. Bossong Raphael. Intelligence Support for EU Security. Options for Enhancing the Flow of Information and Political Oversinght. SWP Comment 2018/C51. December 2018. № 8. P. 1–8.

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

16. Szadeczky Tam s. Information Security Law and Strategy in Hungary. *AARMS.* 2015. № 14 (4). P. 281–289.

17. Helmbrecht Udo. 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. 3 December 2018. P. 1–6.

Анотація

Кавин С. Я. **Правові засади забезпечення кібербезпеки в державах – членах Європейського Союзу.** – Стаття.

Стаття присвячена дослідженню питань правового гарантування інформаційної безпеки, зокрема у сфері кіберзахисту в державах Центрально-Східної Європи в контексті аналізу їхніх національних Стратегій кібербезпеки та відповідних нормативно-правових актів.

У процесі даного дослідження приділено увагу аналізу правових норм, які сприяють ефективному захисту кібербезпеки держави. Аналізуються особливості функціонування інституційно-правового механізму кіберзахисту в контексті законодавчої регламентації міжнародного співробітництва між державними інституціями та структурами національної безпеки. Обґрунтовується необхідність вироблення узгодженої політики кіберзахисту держав Європейського Союзу в контексті інформаційної політики Європейського Союзу з метою уніфікації підходів щодо забезпечення інформаційного захисту та вдосконалення нормативно-правової бази гарантування інформаційної безпеки. Особлива увага приділяється особливостям правового гарантування інформаційної безпеки країн Європейського Союзу в контексті дослідження їхніх національних кіберстратегій як іманентної складової частини національної безпеки, зокрема з погляду диверсифікації зовнішніх відносин у багатовекторній системі міжнародної безпеки.

Проведений аналіз нормативно-правових основ системи кібербезпеки країн Східної та Центральної Європи свідчить про домінантну роль спецслужб у гарантуванні кібернетичної безпеки. У зв'язку із цим міжнародна співпраця стосовно уніфікованих підходів до боротьби з кіберзагрозами в інформаційному просторі має дещо обмежений характер.

Сучасні реалії політики національної безпеки країн Європейського Союзу потребують комплексних досліджень у контексті забезпечення розроблення ефективних механізмів захисту інформаційного простору, дослідження політичних та правових механізмів побудови інформаційної безпеки.

Водночас підходи до інформаційної безпеки, поширені в Європейському Союзі, нині не є уніфікованими. Тому дослідження, оцінка та реалізація позитивного досвіду кожної країни Європейського Союзу в цій сфері важливі під час побудови системи інформаційної безпеки Європейського Союзу.

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

Summary

Kavin S. Y. **Legal framework for cybersecurity in European Union member states.** – Article.

The article is devoted to the study of legal issues of information security, in particular in the field of cyber security in Central and Eastern Europe in the context of the analysis of their national cyber security strategies and relevant regulations.

In the course of this study, attention is paid to the analysis of legal norms that provide effective protection of cybersecurity of the state.

There are analyzed the peculiarities of the functioning of the institutional and legal mechanism of cyber defense in the context of the legislative regulation of international cooperation between state institutions and national security structures. The necessity of developing a coordinated policy of cyber security of the EU country's in order to unify approaches provide to information security and improve the regulatory framework for cyber security is substantiated. Particular attention is paid to the study of regulatory and legal provision of information security in Central and Eastern Europe in the context of studying their national cyber strategies as an inherent component of national security, in particular in terms of diversification of external relations in a multi-vector system of international security.

The analysis of the legal framework of the cybersecurity system in Eastern and Central Europe shows the dominant role of intelligence services in ensuring the cyber security of the state. Therefore, international cooperation on unified approaches to combating cyber threats in the information space somewhat limited in nature.

Accordingly, the current realities of national security policy in EU country's require comprehensive research in the context of the development of effective mechanisms for protecting the information space, the study of political and legal mechanisms for building information security.

However, the approaches to information security adopted in the European Union are currently not unified. Therefore, research, evaluation and implementation of the positive experience of each EU country in this area are important in building the information security system of the European Union.

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