ПРАВОВЕ РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ПРАВІ ЄВРОПЕЙСЬКОГО СОЮЗУ

КАВИН Святослав - Львівський університет імені Івана Франка, аспірант, кафедра європейського права, факультет міжнародних відносин
ORCID: 0000-0002-6189-3848
УДК 341
DOI 10.32782/EP.2022.2.20

Стаття присвячена висвітленню специфіки та особливостей правового регулювання забезпечення інформаційної безпеки в праві ЄС та аналізу основних механізмів правового забезпечення кіберзахисту в контексті дослідження стратегій кібербезпеки ЄС, з метою їх інтеграції в єдину міжнародну багатовекторну систему правового інформаційного простору.

Також увага присвячується вивченню формування ефективної нормативно-правової платформи забезпечення інформаційної безпеки в праві ЄС із мобільним механізмом регулювання кіберзахисту.

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

Постановка проблеми

Важливими тенденціями сучасного етапу розвитку інформаційного суспільства є інтенсифікація транскордонних інформаційних потоків, поширення різноманітних способів і засобів інформаційного обміну, які повною мірою не контролюються ані міжнародними інституціями, ані державами. За цих умов набувають поширення нові кіберзагрози та виклики, що вимагають застосування ефективних нормативно-правових механізмів для відповідного реагування. У зв'язку з цим, пріоритетним питанням на наднаціональному рівні Європейського Союзу є формування уніфікованої правової платформи забезпечення безпеки інформаційного простору.

Міжнародний характер загроз в інформаційному просторі зумовлює необхідність вироблення Європейським Союзом стратегій кібербезпеки та єдиних принципів співробітництва в рамках цієї наднаціональної організації у цій сфері. У той же час у зв'язку з надзвичайно швидким розвитком інформаційних технологій Європейський Союз, стикається все з новими викликами, що вимагає більш швидкого і ефективного реагування. Таким чином, питання правового забезпечення кібербезпеки є вкрай важливими як для Європейського Союзу, так і для кожної держави ЄС на сучасному етапі, що, насамперед, обумовлено необхідністю протистояти протиправним посяганням на інформаційний простір.За цих умов актуальним є комплексне дослідження підходу ЄС до забезпечення кібербезпеки інформаційного простору.

Мета дослідження

Усебічне висвітлення обливостей формування нормативно-правового забезпечення інформаційної безпеки та кібербезпеки в праві ЄС та визначення пріоритетних механізмів регулювання кіберзахисту.

Стан дослідження проблеми

Дослідженню питання забезпечення інформаційної безпеки присвячували у своїх працях ряд вітчизняних та зарубіжних авторів, зокрема В.Шемчук[11], Т.Ткачук, М.Рижков [10], А.Рубан [10], В. Політанський [8], Б. Кормич [7], А. Войцехівський [4], Т.Сліпченко [9], І. Забара [5], М. Василенко [1], [2], [3], В. Маслак [3], Michael Nieles [27],

Kelley Dempsey [27], Victoria Yan Pillitteri [27], Neil Robinson [28], Jan Gaspers [28], Raul A.C. [29], Stahl W. M. [30], Tauwhare R. [31] та інші.

Цікавими в цьому плані є роботи Vytautas Butrimas, зокрема: "Baltic Cyber Cooperation," [33], «The Cybersecurity Dimension of Critical [Energy] Infrastructure (a brief introdauction)» [32]. V. Butrimas своїми багаторічними дослідженнями вніс вагомий вклад у формування системи забезпечення інформаційної безпеки, зокрема в питаннях кіберзахисту критично важливих інфраструктур у контексті міжнародного співробітництва. У своїй доповіді «Cyber threats to critical infrastructure: a new security and defence policy challenge?» на The International Industrial Control System Cyber Security Conference, V.Butrimas переглянув взаємодію між кіберзагрозами для критичної інфраструктури нації та пріоритетами національної оборони, підкресливши зростаючу актуальність міжнародного співробітництва, де нації могли б спільно працювати над управлінням кіберзагрозами і таким чином сприяти їх зменшенню. [34]

Виклад основного матеріалу

В умовах трансформації системи міжнародної безпеки аналіз практики країн ЄС у побудові власних моделей правового забезпечення інформаційної безпеки та протидії кіберзагрозам дає підстави резюмувати про відсутність єдиної моделі правового захисту інформаційного простору в системі права Європейського Союзу. Відповідно, створення ефективного і надійного нормативно-правового механізму забезпечення кібербезпеки європейського інформаційного простору, заснованого на нормах та приципах права Європейського Союзу, є надзвичайно актуальна і очевидна. На жаль, захист інформаційного простору, зокрема критичної іфраструктури від кібератак, досі залишається досить вразливим, виявляючи при цьому проблемні прогалини щодо підвищення надійності стану кібербезпеки в ЄС загалом. У цьому контексті важливо відмітити ряд правових вктів, які були прийняті в рамках удосконалення правового захисту інформаційного простору від кіберзагроз, це: Рамкове рішення Ради ЄС 2005/222/JHA ***щодо нападу на інформаційні системи*** від 24 лютого 2005 р. Це Рамкове рішення має на меті посилити співпрацю між судовими та іншими компетентними органами, у тому числі між поліцейськими та іншими спеціалізованими службами, які уповноважені здійснювати застосування законів у державах ЄС, шляхом зближення їх кримінально-правових норм, яким встановлено мінімальні правила визначення кримінальних злочинів та санкцій у сфері неправомірного впливу на інформаційні системи [15]; Повідомлення Комісії ЄС ***«На шляху до загальної політики у сфері боротьби з кіберзлочинністю» /Towards a general policy on the fight against cyber crime/*** від 22 травня 2007 р., у якому визначено основні напрями політики ЄС щодо інформаційної безпеки, зокрема: стандартизація законодавства країн ЄС та визначень у сфері кіберзлочинності; розробка заходів/індикаторів масштабів кіберзлочинності; політичне та юридичне співробітництво з країнами, що не входять до ЄС через Конвенцію Ради Європи 2001 року про кіберзлочинність (і Додатковий протокол до неї), Ліонську групу G8 щодо високотехнологічних злочинів та проєкти, які керуються Інтерполом; покращення оперативного співробітництва правоохоронних органів шляхом посилення та уточнення відповідальності між Європолом, Євроюстом та іншими структурами; координація взаємопов'язаних навчальних програм для правоохоронних та судових органів країн ЄС із залученням Європолу, Євроюсту, Європейського поліцейського коледжу та Європейської мережі підготовки суддів [25]; Повідомлення Комісії ЄС ***«Захист Європи від широкомасштабних кібератак та руйнувань: посилення рівня підготовленості, безпеки та стійкості» / Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*** / від 30 березня 2009 р., у якому сформовано основні виклики безпеці інформаційних інфраструктур ЄС, а саме: некоординовані національні підходи до безпеки інформаційних інфраструктур; обмежені можливості ЄС щодо раннього попередження та реагування на безпекові інциденти, зумовлені нерозвиненістю міждержавного співробітництва та обміну інформацією щодо цих проблем; відсутність міжнародного консенсусу щодо пріоритетів у

реалізації політики захисту критичної інформаційної інфраструктури. Відповідно в цьому контексті визначено основні заходи для посилення безпеки та здатності європейської критичної інформаційної інфраструктури протистояти зовнішнім впливам [13];

Оскільки проблема захисту кіберпростору є стратегічно важливою, у ЄС було створено Європейське агентство з мережевої та інформаційної безпеки (European Union Agency for Network and Information Security (ENISA)). Спершу ENISA надавало настанови та рекомендації з інформаційної безпеки, а згодом розширило сферу своєї діяльності на вирішення питань кібербезпеки. Сьогодні ENISA виступає центром експертизи як для держав ЄС, так і для інституцій ЄС з отримання консультацій з питань, пов'язаних із мережевою та інформаційною безпекою [12].

Стратегічно важливою подією стало ухвалення у 2013 р. Європейською комісією Стратегії кібербезпеки ЄС ***«Відкритий, надійний та безпечний кіберпростір» /Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace/*** від 07 лютого 2013 р., метою якої було забезпечення відкритого, надійного і безпечного кіберпростору. Прийнята Стратегія рекомендувала державам ЄС розвивати міждержавне співробітництво у протидії кіберзагрозам. Для цього передбачені заходи з наступних напрямків [16];

1) досягнення кіберстійкості;

2) суттєве скорочення кіберзлочинності;

3) розробка політики кібероборони, пов'язаної зі Спільною політикою безпеки і оборони;

4) розвиток виробничих і технологічних ресурсів для кібербезпеки;

5) створення узгодженої міжнародної політики кіберпростору для ЄС і просування його основних цінностей.

А пріоритетами міжнародної політики ЄС у сфері кіберпросторі, як їх визначає Стратегія, стали: [6]:

a) свобода та відкритість: Стратегія визначає принципи користування основоположними правами людини та громадянина у кіберпросторі;

b) застосування законодавства ЄС у кіберпросторі у тій самій мірі, як і у фізичному світі;

c) розвиток потенціалу кібербезпеки через співробітництво з міжнародними партнерами та організаціями, а також громадянським суспільством.

Після оприлюднення Стратегії було розпочато роботу над відповідною директивою. Важливо наголосити, що цей документ розроблявся не окремо від інших напрямків, а як частина ***Стратегії Єдиного Цифрового Ринку (Digital Single Market Strategy)***, з одного боку, і частина ***Європейського Порядку денного з питань безпеки (European Agenda on Security)***, з іншого. [19] Стратегія та Порядок денний були оприлюднені навесні 2015 року, а в липні 2016 року Європейська Комісія презентувала «Додаткові заходи по сприянню розвитку індустрії кіберзахисту».

Також у липні 2016 року була ухвалена Директива Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року про заходи по забезпеченню високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу / ***Directives Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union - NIS Directive/***. [17] Директива закріпила єдині правила та вимоги у сфері кібербезпеки для всіх держав ЄС, але разом з тим залишила за кожною країною ЄС право вживати власних заходів щодо імплементації норм цієї Директиви в національне законодавство з урахуванням національних інтересів [14]. Мета Директиви – це досягнення високого загального рівня безпеки мережевих та інформаційних систем у рамках Європейського Союзу. Разом з тим, Європейська Коміся зазначила, що для досягнення мети Директиви, тобто для забезпечення більш високого рівня мережевої та інформаційної безпеки в межах ЄС необхідно вжити заходів в трьох основних напрямках: [4];

- підвищити спроможність системи кібербезпеки на національному рівні;

- підвищити рівень європейського співробітництва;

- запровадити управління ризиками.

У цьому контексті Директива зобов'язала країни ЄС:

- ухвалити відповідні національні стратегії;

- створювати групи зі співробітництва з метою підтримки і сприяння стратегічній співпраці та обміну інформацією між державами ЄС;

- створювати групи реагування на комп'ютерні інциденти (CSIRT /Computer Security Incident Team/) з метою розвитку довіри між державами ЄС та швидкого й ефективного оперативного співробітництва;

Після створення базової законодавчої платформи у сфері кіберзахисту у вересені 2017 р. Європейська комісія оприлюднила оновлену редакцію Стратегії кібербезпеки. Цей документ був призначений для поліпшення захисту критично важливої інфраструктури Європи і підвищення цифрового самоутвердження ЄС щодо інших регіонів світу. Хоча стратегія і була реформована залежно від динаміки сучасних реалій, однак залишається відкрита низка питань щодо того, як мета стратегії «відкритого, безпечного і надійного кіберпростору» буде надійно захищена як всередині, так і зовні. У ЄС немає ні належним чином певної стабільності або стримування, ні досить ясного пояснення того, як він має намір подолати інституційну фрагментацію і відсутність правових повноважень у питаннях кібербезпеки [18].

При детальнішому аналізі законодавчого пакету ЄС з кібербезпеки можна зазначити наступне: Так, у вересні 2017 року Європейська комісія та Високий представник ЄС із закордонних справ і політики безпеки опублікували спільне повідомлення для Європейського парламенту і Ради ЄС під назвою ***«Стійкість, стримування та захист: створення сильної кібербезпеки для ЄС» /Resilience, Deterrence and Defence: Building strong cybersecurity for the EU/*** від 13 вересня 2017 р., у якому визначається важливість кібербезпеки для розвитку та безпеки держав ЄС і необхідність колективного та широкомасштабного підходу у протидії кіберзагрозам [24]. Це Повідомлення стало частиною пакету документів ЄС, спрямованих на забезпечення більш сильного реагування ЄС на кібератаки. Зокрема, Спільне повідомлення передбачає цілеспрямовані заходи, скеровані на створення більшої стійкості ЄС до кібератак, а також краще виявлення кібернападів і посилення міжнародної співпраці у сфері кібербезпеки. У документі викладені заходи, спрямовані на підвищення кіберстійкості ЄС, зокрема: ***швидке прийняття нового Регламенту ЄС***, який реформує Агентство ЄС з кібербезпеки (ENISA). У вересні 2017 року Комісія прийняла пакет з кібербезпеки з новими ініціативами щодо подальшого покращення кіберстійкості ЄС, стримування та оборони. У рамках цих заходів Комісія внесла законодавчу пропозицію щодо посилення Агентства ЄС з інформаційної безпеки мережі (ENISA). [22] Відповідно ENISA відіграватиме більш широку роль у ландшафтному середовищі ЄС у сфері кібербезпеки, але вона обмежена поточним мандатом та ресурсами. Комісія представила амбітну пропозицію про реформу, включаючи постійний мандат агентства, щоб гарантувати, що ENISA може не лише надавати експертні консультації, а й виконувати оперативні завдання. Пропозиція також передбачала створення першої добровільної системи сертифікації кібербезпеки в ЄС для продуктів ІКТ, де ENISA також відіграватиме важливу роль. Нове положення набуло чинності 27 червня 2019 року. [19]; ***узгодження спільної галузевої ініціативи*** щодо єдиного ринку кібербезпеки. Відсутність визнаних у ЄС схем сертифікації кібербезпеки для встановлення більш високих стандартів стійкості до продуктів та підкріплення довіри ринку в ЄС спонукала Комісію висунути пропозицію щодо створення системи сертифікації кібербезпеки ЄС. Згідно з цією ініціативою визначатиметься процедура створення загальноєвропейських схем сертифікації кібербезпеки, що охоплює продукти, послуги та/або системи, які адаптують рівень гарантій до використання; ***повна та ефективна імплементація Директиви ЄС про безпеку мережних та інформаційних систем («Директива NIS»)*** усіма державами ЄС. Загрози кібербезпеки майже завжди є транскордонними, і кібератака на критично важливі об'єкти однієї країни може вплинути на ЄС у цілому. Тому державам ЄС необхідно мати сильні урядові органи, які здійснюють нагляд за кібербезпекою у своїй країні, особливо у сек-

торах, що мають вирішальне значення для суспільства, та працювати разом зі своїми колегами в інших державах ЄС шляхом обміну інформацією. Відповідно, вони домовилися з ЄС забезпечити це шляхом прийняття NIS Directive (Directive on security of Network and Information Systems) [17] У результаті процесу розгляду Комісією 16 грудня 2020 року було представлено пропозицію у відповідності до директиви щодо заходів для високого загального рівня кібербезпеки в Союзі (NIS2 Directive) [26]. Швидка реалізація «Концепції» для транскордонного реагування на великі інциденти. «План» був представлений у Рекомендації ЄС і визначає цілі та способи співпраці між державами ЄС, а також між державами ЄС та відповідними інституціями ЄС, у відповідь на масштабні інциденти та кризові ситуації у сфері кібербезпеки. Розробка єдиного порталу – єдиного в масштабах ЄС – який буде надавати інформацію про останні кіберзагрози і об'єднувати практичні поради та інструменти кібербезпеки для допомоги жертвам кібератак тощо. [9]

2019 року був прийнятий Регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій, а також про скасування Регламенту (ЄС) № 526/2013 (Акт про кібербезпеку) ***/Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)/*** [23]. У ньому закладено основні положення щодо ENISA, зокрема ENISA призначена як постійне агентство ЄС з кібербезпеки та структури для створення європейських схем сертифікації кібербезпеки з метою забезпечення адекватного рівня кібербезпеки продуктів і послуг ІКТ в ЄС. Регламент створює нові механізми для розвитку європейської стратегічної автономії. Разом з тим, Регламент має подвійну мету: по-перше - прийняття постійного мандата ENISA; по-друге - визначення Європейської основи сертифікації у сфері кібербезпеки. І перше і друге мають важливе значення для підвищення безпеки Європейського єдиного цифрового простору.

У грудні 2020 р. Європейська Комісія та Верховний представник Європейського Союзу з питань закордонних справ і політики безпеки представили ***Стратегію кібербезпеки Євросоюзу на цифрове десятиліття (The EU's Cybersecurity Strategy, 2020)***. Стратегія містить конкретні пропозиції щодо розгортання таких трьох основних інструментів у сфері міжнародного інформаційного співробітництва як регуляторний, інвестиційний та політичний. Ці інструменти є необхідними і важливими для забезпечення трьох сфер дій ЄС у питаннях захисту інформаційного простору від кібератак, зокрема: [20]

– стійкість, технологічний суверенітет та лідерство;

– нарощування оперативного потенціалу для запобігання, стримування та реагування;

– просування глобального та відкритого кіберпростору.

ЄС прагне підтримувати цю стратегію шляхом безпрецедентного рівня інвестицій у цифрову трнсформацію простору ЄС.

Стратегія кібербезпеки Євросоюзу на цифрове десятиліття спрямована на зміцнення колективної стійкості Європи проти кіберзагроз.

Серед нових стратегічних ініціатив Євросоюзу доцільно виділити такі: – створення Європейського кіберщита (An EU-wide Cyber Shield) через мережу Операційних центрів безпеки (Security Operations Centres, SOCs) з підтримкою штучного інтелекту; – створення Спільного кіберпідрозділу (A Joint Cyber Unit) – платформи з кооррдинаційними функціями для ефективного захисту Європейський Союз від транскордонних кібератак; розроблення положення про високі стандарти кібер- та інформаційної безпеки Європейського Союзу.

Зусиллями ЄС планується підтримувати розробку законодавства та політики країн-партнерів згідно з відповідною політикою та стандартами ЄС у галузі кібердипломатії.

У березні 2021 р. Європейська Рада прийняла висновки щодо Стратегії кібербезпеки Європейського Союзу на цифрове десятиліття, у яких зазначається, що кібербезпека

має важливе значення для побудови стійкої, зеленої та цифрової Європи (Cybersecurity: Council adopts, 2021). [21] Зазначені висновки ставлять ключовою метою досягнення стратегічної автономії при збереженні відкритої економіки, з метою зміцнення цифрового лідерства та стратегічного потенціалу Європейського Союзу. Разом з тим Європейська Рада наголошує на необхідності підтримки розвитку надійного шифрування як засобу захисту основних прав і цифрової безпеки, забезпечуючи при цьому здатність правоохоронних і судових органів здійснювати свої повноваження як у мережі, так і в автономному режимі.

Висновки

Для забезпечення надійного захисту інформаційного простору від несанкціонованого доступу та кібератак одним з головних приорітетів ЄС мала б стати розробка на наднаціональному рівні нормативно-правових актів, які встановлюють перелік злочинів в ІТ-сфері, а також встановлюють кримінальну відповідальність за злочини в ІТ-сфері із використанням інформаційно-комунікаційних технологій.

Важливою особливістю підходу ЄС у сфері інформаційної безпеки є послідовна і цілеспрямована політика, спрямована на знаходження балансу між національною і наднаціональною компетенціями. Загальноєвропейські структури, як правило, не підміняють собою національні відомства, а є координуючими центрами, надають інформаційну, експертну і технічну підтримку.

У зв'язку з надзвичайною актуальністю безпеки інформаційного простору, в інститутах Європейського Союзу сформувалось концептуальне бачення майбутнього міжнародно-правового регулювання забезпечення інформаційної безпеки, яке полягає в попередженні кримінальних злочинів, пов'язаних із використанням інформаційно-комунікаційних технологій. У цьому контексті важливим є формування в рамках правової платформи ЄС концепції міжнародної інформаційної безпеки, яка передбачала б комплексне вирішення проблеми.

Література

1. Василенко М. Підвищення стану кібербезпеки інформаційно-комунікаційних систем: якість в контексті удосконалення інформаційного законодавства / М. Василенко // Юридичний вісник. – 2018. – № 3. –- С. 17–24.

2. Василенко М. Якість кібербезпеки інформаційно-комунікаційних систем (ІКС) та деякі законодавчі питання щодо її підвищення / М. Василенко // Юридичний вісник. – 2018. – № 4.

3. Василенко Д.П., Маслак В.І. Законодавство провідних країн світу в сфері захисту інформації. Вісник КДУ імені Михайла Остроградського. Випуск № 61, частина 1. Частина 1. С.128-132.

4. Войцехівський А.В. Кібербезпека як важлива складова системи захисту національної безпеки європейських країн. Журнал східноєвропейського права. 2018- № 53 С.26-37

5. Забара І.М. Формування сучасних правових засад кібернетичної безпеки Європейського Союзу в умовах поширення нових інноваційних технологій. Журнал європейського і порівняльного права. 2017. Вип. 3. С. 2-13.

6. Законодавство та стратегії у сфері кібербезпеки країн Європейського Союзу, США, Канади та інших URL: https://clck.ru/FEMKX. (дата звернення: 10.01.2022).

7. Кормич Б.А. Інформаційна безпека: організаційно-правові основи [Текст] : навч. посібник для студ. вищих навч. закл. /- Б.А. Кормич. – К. : Кондор, 2004. – 384 с. – (Юридична книга). [Kormych B. 2004. Information Security: Organizational-Legal Basis. Kiev: Condor.]

8. Політанський В.С. Світові моделі та фундаментальні принципи інформаційного суспільства. Науковий вісник Ужгородського національного університету: серія «Право». Випуск 43, том 1. 2017. С.3439

9. Сліпченко Т. Кібербезпека як складова системи захисту національної безпеки: європейський досвід. (Online) Актуальні проблеми правознавства 2020 № 1 (21)

10. Рижков М. М., Рубан А. Стратегія інформаційної і кібербезпеки ЄС: сучасний вимір. Міжнародні відносини. Серія «Політичні науки». 2019. № 21. URL: http://ournals.iir.kiev.ua/index.php/pol_n/article/view/3866 (дата звернення: 10.01.2022).

11. Шемчук В.В. Зарубіжний досвід забезпечення інформаційної безпеки держави

// Порівняльне-аналітичне право. 2019. Вип. № 2. С. 188–191.

12. About ENISA / European Union Agency for Network and Information Security URL : https://www.enisa.europa.eu/about-enisa. (дата звернення: 10.01.2022).

13. Communication from the Commission on Critical Information Infrastructure Protection «Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience»: adopted by the European Commission on 30 March 2009 / European Union. URL: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A52009DC0149 (дата звернення 10.01.2022).

14. Concerning measures for a high common level of security of network and information systems across the Union - NIS Directive: Directive (EU) 2016/1148 of the European parliament and of the council of 6 July 2016 / Official Journal of the European Union. URL: http://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (дата звернення 01.01.2022).

15. Council framework decision 2005/222/JHA on attacks against information systems: adopted by the Council of the European Union on 24 February 2005 / European Union. URL:https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX:32005F0222 (дата звернення 10.01.2022).

16. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace: adopted by the European Commission on 7 February 2013 / European Union. URL: https://ec.europa.eu/digital-singlemarket/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cybersecurity (дата звернення 10.01.2022).

17. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union // Official Journal of the European Union. – 2016. – L. 194. – P. 1–30. URL:https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN (дата звернення 10.01.2022).

18. ENISA and a new cybersecurity act. European Parlament URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/614643/EPRS_BRI(2017)614643_EN.pdf (дата звернення 10.01.2022).

19. EU cybersecurity initiatives working towards a more secure online environment / European Union.

URL:http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf

(дата звернення 10.01.2022).

20.European Commission. The EU's Cybersecurity Strategy for the Digital Decade. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN (дата звернення: 10.01.2022).

21.European Council. Cybersecurity: Council adopts conclusions on the EU's cybersecurity strategy. URL: https://www.consilium.europa.eu/en/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy (дата звернення: 10.01.2022).

22.Proposal for a regulation of the European Parliament and of the Council on ENISA, the «EU Cybersecurity Agency», and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification («Cybersecurity Act») URL : https://clck.ru/FEMLA. (дата звернення: 10.01.2022).

23.Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act. Text with EEA relevance).

URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32019R0881 (дата звернення: 10.01.2022).

24.Renewed Cybersecurity Strategy: European Parliament and Council Joint Communication 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU' (JOIN (2017) 450) URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN (дата звернення: 10.01.2022).

25.Towards a general policy on the fight against cyber crime: adopted by the European Commission on 22 May 2007 / European Union. URL: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=LEGISSUM%3Al14560 (дата звернення 10.01.2022).

26.The NIS2 Directive. A high common level of cybersecurity in the EU. European Parlament URL:https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf (дата звернення: 10.01.2022).

27.Michael Nieles, Kelley Dempsey and Victoria Yan Pillitteri. 2017. An Introduction to Information Security. Special Publication 800-12 Revision 1. Gaithersburg: National Institute of Standards and Technology (NIST)

28.Neil Robinson and Jan Gaspers. 2014. Information Security and Data Protection Legal and Policy Frameworks Applicable to European Union Institutions and Agencies. Brussels: RAND Corporation

29.Raul A. C. (ed.). The privacy, data protection and cybersecurity law review. – Law Business Research Limited, 2018.

30.Stahl W. M. The uncharted waters of cyberspace: applying the principles of international maritime law to the problem of cybersecurity // Ga. J. Int'l & Comp. L. – 2011. – T. 40. – C. 247.

31.Tauwhare, R. (2016). Improving cybersecurity in the European Union: the Network and Information Security Directive. Journal of Internet Law, 19(2), 1–12.

32.Vytautas Butrimas. Baltic Cyber Cooperation, per Concordiam: Journal of European Security Defense Issues 7, No. 2, 2016: 18-23.

33.Vytautas Butrimas. The Cybersecurity Dimension of Critical [Energy] Infrastructure (a brief introdauction), NATO Energy Security Centre of Excellence ESET, Vilnius 2019

34.V. Butrimas (Chief Adviser of the Ministry of National Defence) delivered an announcement at the international Industrial Control System Cyber Security Conference URL:

http://kam.lt/en/news_1098/news_archives/news_archive_2012/news_archive_2012__10/chief_adviser_of_the_ministry_of_national_defence_v._butrimas_delivered_an_announcement_at_the_international_industrial_control_system_cyber_security_conference.html (дата звернення: 10.01.2022).

Sviatoslav Kavyn

LEGAL REGULATION OF INFORMATION SECURITY IN THE LAW OF THE EUROPEAN UNION

The paper highlights the specifics and features of the legal regulation of information security in EU law. The main mechanisms of legal support of cyber defense in the context of the study of EU cyber security strategies are analyzed, in order to integrate them into a single international multi-vector system of legal information space. In this context, the peculiarities of the formation of regulatory and legal support for information security and cybersecurity in EU law are studied, on the basis of which the priority mechanisms for regulating cybersecurity are determined. Particular attention is paid to the study of the formation of an effective regulatory platform for information security in EU law with a mobile mechanism for regulating cybersecurity at the supranational level in the context of the specifics of national legislation.

Research shows that in order to ensure reliable protection of the information space from unauthorized access and cyber attacks, one of the EU's top priorities should be the development at the supranational level of regulations establishing criminal liability for IT crimes using information and communication technologies. It also emphasizes the important feature of the EU's approach to information security, which is a consistent and focused policy aimed at finding a balance between national and supranational competencies. It is noted the conceptual vision of the future international legal regulation of information security, which consists in the prevention of criminal offenses related to the use of information and communication technologies. In this context, it is important to form within the EU legal platform the concept of international information security, which would provide a comprehensive solution to the problem.

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