Nasylstvo yak katehoriia zahalnoi chastyny vchennia pro obstavyny, shcho vykliuchaiut zlochynnist diiannia. *Visnyk Kharkivskoho natsionalnoho universytetu imeni V. N. Karazina.* Seriia «Pravo». 2019. 27. S. 89. **21.** Sobko H. M. Psykhichne nasylstvo yak obstavyna, shcho vykliuchaie zlochynnist diiannia. *Pidpryiemnytstvo, hospodarstvo i pravo.* 2019. № 10. S. 152.

Kvasha Roman, Feshchenko Oleh. **Physical and mental violence as the main types of criminal violence**

The article states that there is no clear differentiation of types of violence either in domestic legislation or in criminal law science. The following are defined as objective and subjective signs of violence: illegal behavior that manifests itself in the external environment and is expressed in specific conscious acts of human activity; targeting another person's body; the presence of a specific addressee (the victim – in the case of direct violence, or his relatives – in the case of indirect violence); can take place both against and against the will of another person (victim); the intentional character of the person's behavior; the ability to influence the unconscious and cause physical, moral, property damage to another person; the presence of a goal to cause harm to another person of a certain nature.

The dominant position is the division of violence into physical and mental. An objection was expressed against the existence of formulas: «violence = physical violence», «threat = mental violence» (this is exactly the vision of the developers of the new Criminal Code of Ukraine). This approach, in contrast to the generally accepted division of violence into physical and mental, determines the thesis that violence exists exclusively in the form of physical harm to the victim, and reduces another type of violence, mental, to a threat. Whereas mental violence in the current Criminal Code of Ukraine manifests itself not only through threats, but also coercion, coercion, influence, terrorizing, etc. The thesis that physical violence can manifest itself not in active actions, but in the form of inaction, has been criticized. However, even examples simulated by scientists refute this approach. It is supported by the idea that murder is also a manifestation of violence, since it is committed in a violent way, at the same time, violence does not include the destruction and damage of someone else's property. Although physical violence is traditionally considered the most dangerous, in some cases mental violence can cause irreparable damage to a person's health. Signs of mental violence as a deliberate, criminally illegal and socially dangerous act are also the active nature of the behavior (as in the case of physical violence), the influence on the psyche of another person against their will, as a result of which harm is caused to the health or life of a person.

Key words: *violence, aggression, physical violence, mental violence, psychological violence, types of violence, threat, harm, murder, destruction of property, action, inaction, influence, intimidation.*

Розділ VII

ПРОБЛЕМИ МІЖНАРОДНОГО ПРАВА ТА ПОРІВНЯЛЬНОГО ПРАВОЗНАВСТВА

DOI: 10.33663/0869-2491-2024-35-667-682
УДК 341.171

Л. Г. ФАЛАЛЄЄВА,
*доктор юридичних наук**
ORCID: 0000-0001-6089-2459

Б. В. СТРІЛЕЦЬ,
*кандидат юридичних наук***
ORCID: 0000-0001-7043-7329

ПАРАДИГМА КІБЕРБЕЗПЕКИ У ПРАВІ ЄВРОПЕЙСЬКОГО СОЮЗУ: СУЧАСНІ РЕАЛІЇ В УМОВАХ ЦИФРОВІЗАЦІЇ

Дослідження присвячено аналізу сучасної парадигми кібербезпеки у праві Європейського Союзу в умовах цифровізації. Висвітлено доктринальні підходи до визначення кібербезпеки у рамках цього інтеграційного об'єднання. Проаналізовано акти ЄС, у яких робиться акцент на важливості кібербезпеки для забезпечення функціонування внутрішнього ринку ЄС, а не забезпечення дотримання прав людини, передусім основоположних прав, що не можна вважати виправданим.

Автори статті віддають перевагу широкому підходу до визначення кібербезпеки у праві ЄС. У такому випадку можливе формування права на кібербезпеку, яке включає не лише стан технічної захищеності, а також належні правові та інституційні гарантії захисту і відшкодування заподіяної шкоди. Зроблено висновок про те, що закріплення права на кібербезпеку у праві ЄС, а також сучасні реалії цифровізації, вимагають трансформації структури та повноважень Агентства Європейського Союзу з кібербезпеки (ENISA).

* ***Falalieieva Liudmyla****, Doctor of Juridical Sciences*
** ***Strilets Bohdan****, Candidate of Juridical Sciences (Ph. D)*

Ключові слова: *право ЄС, акти ЄС, громадяни ЄС, кібербезпека, кіберзахист, цифровізація, інформаційно-комунікаційні технології, внутрішній ринок ЄС, свобода руху капіталу в ЄС, європейська інтеграція.*

Falalieieva Liudmyla, Strilets Bohdan. **Paradigm of cybersecurity in European Union law: modern realities in the context of digitalisation**

The study analyses the current paradigm of cybersecurity in the law of the European Union in the context of digitalisation. The authors highlight the doctrinal approaches to the definition of cybersecurity within this integration association. They analyse the EU acts which emphasise the importance of cybersecurity for ensuring the functioning of the EU internal market rather than ensuring the observance of human rights, especially fundamental rights, which cannot be considered justified.

The authors prefer a broad approach to the definition of cybersecurity in EU law. In this case, it is possible to formulate the right to cybersecurity, which includes not only the state of technical security, but also appropriate legal and institutional guarantees of protection and compensation for damage. It is concluded that introducing the right to cybersecurity into EU law, as well as the current realities of digitalisation, require a transformation of the structure and powers of the European Union Agency for Cybersecurity (ENISA).

Key words: *EU law, EU acts, EU citizens, cybersecurity, cyber defence, digitalisation, information and communication technologies, EU internal market, free movement of capital in the EU, European integration.*

Постановка проблеми. Трансформація повсякденного життя у цифрові формати, що охоплює приватні та публічні правовідносини, очевидна. Цифровізація спрямована на підвищення рівня життя, оптимізацію економічних процесів, особливо транскордонного характеру, та підвищення ефективності державних послуг. Вона також є надважливою для динамічного розвитку внутрішнього ринку Європейського Союзу (далі – ЄС), на якому забезпечується вільний рух товарів, осіб, послуг, а також свобода руху капіталу. Цифровізація останнього відбувається відповідно до Стратегії єдиного цифрового ринку для Європи 2015 р. Стратегія окреслює цілі, серед яких покращення доступності товарів і послуг онлайн по всій Європі як для споживачів, так і для бізнесу, створення якомога більше сприятливого середовища для функціонування цифрових мереж і послуг, а також розкриття повного потенціалу зростання цифрової економіки Європи[1].

Стрімке зростання цифрової економіки потребує адекватного правового регулювання не лише для її розвитку, а й для захисту всіх суб'єктів, які беруть участь у правовідносинах у цифровому середовищі. Кожну хвилину, навіть секунду, використання інформаційно-комунікаційних технологій (далі – ІКТ) переплітається з кіберризиками, що потребує швидких і правильних дій, постійних зусиль для створення безпечного кіберсередовища. Нехтування цим може поставити під загрозу як функціонування внутрішнього ринку ЄС, так і стабільність самого інтеграційного об'єднання, особливо в контексті посилення кіберзагроз з боку російської федерації. Як зазначено

у преамбулі Регламенту (ЄС) 2019/881 Європейського Парламенту та Ради ЄС від 17 квітня 2019 р. про ENISA (Агентство Європейського Союзу з кібербезпеки) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій і скасування Регламенту (ЄС) № 526/2013 (далі – Акт про кібербезпеку ЄС), кіберзагрози не мають кордонів і є глобальною проблемою[2].

Станом на початок 2024 р. у ЄС було ухвалено низку правових актів, спрямованих на зміцнення цифрової безпеки та сприяння спільним зусиллям держав – членів інтеграційного об'єднання у цій сфері. Незважаючи на ці ініціативи, зростає занепокоєння щодо ефективності правових та інституційних механізмів ЄС у вирішенні сучасних викликів цифровій безпеці. Звіти Європолу (Агентства ЄС зі співробітництва у правоохоронній сфері) свідчать про активізацію кіберзлочинності, про появу нових кіберзлочинів. Серед останніх переважають випадки онлайн-шахрайства, несанкціонованого отримання персональних даних і відмивання коштів за допомогою як традиційних, так і цифрових валют[3] (під першими розуміють євро та ін., а під другими – Bitcoin, Ethereum і т. д.). Водночас простежується брак знань про кібербезпеку серед громадян ЄС та європейських компаній[4]. Зазначена негативна тенденція підкреслює необхідність постійної оцінки та адаптації стратегій кібербезпеки ЄС для ефективної протидії еволюціонуючим цифровим загрозам.

Окремі аспекти правових засад регулювання кібербезпеки в ЄС розглядались у працях вітчизняних учених, зокрема І. Батько, А. Грубінка, О. Звоздецької, А. Семенченка, а також зарубіжних науковців, серед яких А. Бендіек, Н. Гамал, О. Гамуляк, П. Мазуріер, Л. Мартіно, В. Папаконстантіноу, Н. Шишкова та ін. Однак комплексного дослідження правового регулювання кібербезпеки у ЄС і системного аналізу тенденцій його розвитку в сучасних реаліях стрімкої еволюції цифрових технологій не проводилося. Відтак метою статті є осмислення та аналіз сучасної парадигми кібербезпеки у праві ЄС в умовах цифровізації.

Виклад основного матеріалу дослідження. У 2013 р. Стратегія кібербезпеки ЄС (далі – Перша Стратегія кібербезпеки) була опублікована як Спільне повідомлення для Європейського Парламенту, Ради ЄС, Європейського економічного і соціального комітету та Комітету регіонів. Вона окреслила основні пріоритети та напрями формування єдиної європейської системи кібербезпеки. У ній замість поширеного на той час терміна «мережева та інформаційна безпека» (перший документ Європейської Комісії «Мережева та інформаційна безпека: пропозиція щодо підходу до європейської політики» з'явився у 2001 р.[5]) уперше вживається термін «кібербезпека». Щоправда, автори Стратегії не наважилися дати його чіткого визначення. Вочевидь це пов'язано з тим, що на той час інституції ЄС не були готові віддати перевагу одному з багатьох концептуальних підходів до сутності кібербезпеки та кіберзагроз. З одного боку, поспішні формулювання у будь-якому випадку не мали б вирішального значення, а з іншого – пові-

домлення, згідно з установчими договорами ЄС, не належать до правових інструментів реалізації європейської інтеграції.

Акт про кібербезпеку ЄС став фундаментальним орієнтиром, який сформував основні інституційні та правові гарантії безпеки для учасників правовідносин у цифровому середовищі на рівні ЄС. Не менш важливим є те, що ст. 2 Акта про кібербезпеку ЄС визначає кібербезпеку як діяльність, необхідну для захисту мережевих та інформаційних систем, користувачів таких систем та інших осіб, на яких впливають кіберзагрози. Останні включають будь-яку потенційну обставину, подію або дію, яка може пошкодити, порушити або іншим чином негативно вплинути на мережеві та інформаційні системи, користувачів таких систем та інших осіб[6]. Проте докладне визначення кібербезпеки у праві ЄС не поклало край дискусіям щодо її сутності та значення для внутрішнього ринку ЄС, приватних правовідносин громадян ЄС, безпеки держав-членів і самого інтеграційного об'єднання як актора міжнародних відносин і суб'єкта міжнародного права. Однією з причин наведеного є те, що Акт про кібербезпеку ЄС є насамперед установчим актом Агентства Європейського Союзу з кібербезпеки (далі – ENISA) та основою для європейської системи сертифікації кібербезпеки, а не систематизацією прав та обов'язків, як можна було б очікувати, зважаючи на гучну назву законодавчого акта.

Варто враховувати, що надати вичерпну та всеохопну характеристику кібербезпеці як такій, майже неможливо. Доктринальні розбіжності призвели до того, що кібербезпеку можна розглядати як мінімум з трьох позицій: як заходи та дії, спрямовані на захист інформаційних систем; як стан захищеності кіберсередовища; врешті, як здатність захищатись і протистояти наявним і потенційним загрозам[7]. Так, Кембриджський словник пропонує розглядати кібербезпеку як заходи, що застосовуються для захисту людини, організації чи держави та їх комп'ютерної інформації від злочинів чи атак, вчинених з використанням Інтернету[8]. Погляд на кібербезпеку з точки зору «стану», а не «заходів / дій» дав підстави деяким вченим для висновку, що вона полягає у захищеності систем, підключених до Інтернету, зокрема обладнання, програмного забезпечення та даних, від кібератак[9]. Однак поділяємо позицію В. Папаконстантіноу, який схиляється до дихотомії кібербезпеки як стану захищеності та заходів, спрямованих на такий захист[10]. Саме такій концепції цілком відповідає чинне законодавче визначення кібербезпеки на рівні ЄС. Акт про кібербезпеку ЄС розкриває її водночас і як стан захищеності, оскільки всі суб'єкти мають право на захист від «будь-яких потенційних обставин, подій чи дій», які можуть мати несприятливий вплив, і як практику («дії, необхідні для захисту» суб'єктів чи об'єктів, яким загрожують кіберзагрози)[11]. Щоправда, такі ідеї не набули подальшого розвитку в законодавстві ЄС, хоча логічно випливають із закладених у Акті про кібербезпеку ЄС базових ідей і принципів кібербезпеки. Опубліковане у грудні 2020 р. «Спільне повідомлення: Стратегія кібербезпеки ЄС на цифрове десятиліття»12 (далі – Друга Стратегія кібербезпеки) теж не містить завдань і цілей, що вписуються в наведену парадигму.

Стан захищеності у кіберпросторі (середовищі, яке функціонує за допомогою комп'ютерних систем, надаючи можливості для здійснення комунікацій та/або реалізації суспільних відносин) може існувати виключно в поєднанні з правом людини на кібербезпеку. Таке право реалізується через правові та інституційні гарантії захисту прав учасників правовідносин у цифровому середовищі. Однак Акт про кібербезпеку ЄС, як і Перша та Друга Стратегії кібербезпеки, роблять акцент на важливості кібербезпеки для забезпечення функціонування внутрішнього ринку ЄС, а не захисту прав людини. Цифровий світ розглядається здебільшого через економічну призму з точки зору вільної торгівлі. Критичною у цьому контексті є Директива (ЄС) 2016/1148 Європейського Парламенту та Ради ЄС від 6 липня 2016 р. про заходи для забезпечення високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу,13 яка має на меті, згідно зі ст. 1.1, покращення функціонування внутрішнього ринку ЄС. Без сумніву, будь-які безпекові прогалини можуть мати неконтрольовані наслідки для внутрішнього ринку ЄС, підриваючи основи функціонування цього інтеграційного об'єднання. Проте бачення захисту прав людини, передусім основоположних прав, як другорядної складової кібербезпеки вочевидь не можна вважати виправданим.

Акцентування уваги саме на необхідності забезпечення функціонування внутрішнього ринку має також логічну правову, можливо, й політичну першопричину. Відповідно до принципу субсидіарності у сферах, що не належать до його виключної компетенції, ЄС діє лише якщо та у такому обсязі, в якому держави-члени не можуть належним чином досягти цілей запропонованого заходу на центральному, регіональному або місцевому рівнях, а натомість це краще здійснити на рівні Союзу з огляду на масштаби або результати запропонованих заходів (ст. 5 (п. 3) Договору про Європейський Союз у редакції Лісабонського договору 2007 р.)14 Захист прав людини здебільшого залишається у площині повноважень держав-членів, водночас правове регулювання внутрішнього ринку ЄС потребує консолідованих зусиль на загальносоюзному рівні. Формулювання, що використовуються у Директиві (ЄС) 2016/1148 від 6 липня 2016 р., свідчать переважно не про ігнорування необхідності захисту прав людини у кіберпросторі, а про обґрунтування необхідності правового регулювання цієї сфери на рівні ЄС.

Отже, кібербезпеку цілком можна розглядати з точки зору особистої недоторканності громадян ЄС у кіберпросторі. Право на особисту недоторканність є одним з основоположних прав людини, гарантованих ст. 3 Загальної декларації прав людини, ст. 5 Конвенції про захист прав людини і основоположних свобод, ст. 6 Хартії Європейського Союзу про основоположні права. Приватні правовідносини у кіберпросторі набувають повсяк-

денного характеру, тому їх захист від посягань є одним із важливих завдань у реаліях сьогодення.

Враховуючи викладене, маємо підстави стверджувати, що кібербезпека має приватну та публічну складові. Перша стосується забезпечення прав громадян ЄС на безпечне кіберсередовище і, як наслідок, безперешкодний доступ до соціальних благ і до вільної економічної діяльності в межах внутрішнього ринку ЄС. Друга полягає у забезпеченні безпеки держав – членів та інтеграційного об'єднання в цілому, становлячи важливу складову їх оборонної діяльності, здійснюваної у рамках Спільної безпекової та оборонної політики ЄС.

Приватна складова кібербезпеки охоплює надзвичайно широке коло правовідносин. Принаймні частину з них покликаний врегулювати Акт про кібербезпеку ЄС. Правові гарантії кібербезпеки, запроваджені цим законодавчим актом, зводяться до встановлення схем сертифікації. Їх дія має гарантувати, що продукти, послуги та процеси, в яких використовуються ІКТ, відповідають встановленим вимогам безпеки. Оскільки кібербезпека невід'ємно пов'язана з усіма цифровими продуктами, послугами та процесами, європейська сертифікація має усі шанси на те, щоб стати ключовим інструментом для підтримки стратегічної автономії європейського кіберпростору[15]. Вона скерована на забезпечення його стабільного функціонування та формування суспільної довіри до нього. Одночасно дієва система сертифікації здатна зобов'язати іноземних провайдерів і треті країни дотримуватись схем для доступу до внутрішнього ринку ЄС.

Акт про кібербезпеку ЄС майже обходить стороною відповідальність суб'єктів сертифікації у випадку недотримання європейських і міжнародних стандартів. Проте якщо проблема притягнення до відповідальності за необхідності може бути вирішена державами-членами, то реальною прогалиною Акта про кібербезпеку ЄС є те, що він не окреслює обсягу прав чи засобів захисту осіб, права яких будуть у такому випадку порушені.

Значний крок уперед у цьому сенсі було зроблено з прийняттям Регламенту (ЄС) 2022/2554 Європейського Парламенту та Ради ЄС від 14 грудня 2022 р. про цифрову операційну стійкість для фінансового сектору та внесення змін до Регламентів (ЄС) № 1060/2009, (ЄС) № 648/2012, (ЄС) № 600/2014, (ЄС) № 909/2014 та (ЄС) 2016/1011, в якому визначено систему нагляду за постачальниками ІКТ послуг[16]. Однак сфера дії цього правового акта надзвичайно обмежена і стосується лише основних аспектів фінансової діяльності з використанням ІКТ. Скажімо, він приділяє мінімальну увагу правовідносинам, пов'язаним із криптовалютами (емісія, обіг, інвестиційна діяльність, обмін тощо). Враховуючи, що капіталізація ринку криптовалют перевищує 1,5 трильйона доларів США, його вплив на приватні фінансові відносини громадян ЄС, а також на внутрішній ринок інтеграційного об'єднання не може бути непоміченим. Саме він цілком може стати основою функціонування єдиного цифрового ринку ЄС. При цьому ринок криптовалют існує

виключно у кіберпросторі, а тому будь-яке втручання у безпеку криптовалютних операцій є ні чим іншим, як кіберзагрозами. Кібербезпека у цій сфері, яку умовно можна позначити як «криптобезпека», на нашу думку, потребує окремого правового регулювання з огляду на специфіку криптоактивів і криптовалютного ринку в цілому, до якої віднесемо: значну волатильність (коливання цін); функціонування насамперед на основі технології блокчейн (розподіленої бази даних, що зберігає впорядкований ланцюжок записів – «блоків»); надзвичайно велику кількість криптовалют[17], частина з яких не мають визначеного правового статусу / режиму[18]; більші можливості для анонімності порівняно зі звичайною банківською сферою; нові можливості для шахраїв у контексті виманювання криптоактивів у користувачів[19] тощо.

Регламент 2022/2554 у більшості випадків віддає перевагу відсильним нормам, які делегують правове регулювання Регламенту (ЄС) 2023/1114 Європейського Парламенту та Ради ЄС від 31 травня 2023 р. про ринки криптоактивів і внесення змін до Регламентів (ЄС) № 1093/2010 і (ЄС) № 1095/2010 та Директив 2013/36/ЄС і (ЄС) 2019/1937[20]. Аналіз положень останнього вказує на те, що він лише частково зачіпає питання кібербезпеки і здебільшого спрямований на фінансовий контроль за діяльністю емітентів криптоактивів. На них покладаються обов'язки діяти чесно і професійно, підтримувати всі свої системи та протоколи доступу згідно з відповідними стандартами ЄС, повернути покупцям або потенційним покупцям будь-які зібрані кошти у разі скасування емісії тощо.

У 2022 р. Європейські наглядові органи (Європейське банківське управління, Європейське управління з цінних паперів та ринків і Європейське управління зі страхування та професійних пенсій) зробили спільну заяву щодо загроз, з якими можна зіткнутися під час використання криптоактивів[21]. У цей час ENISA віддає у своїй роботі перевагу розкриттю саме технічних аспектів існування ринку криптовалют[22]. Наведене свідчить про те, що, незважаючи на суто цифровий характер взаємодії з криптоактивами, інституції ЄС не відносять загрози учасникам крипторинку до кіберзагроз. Примітно, що однією із загроз, про яку не йдеться у зазначеній заяві Європейських наглядових органів[23] є глобальна загроза з боку держав – спонсорів тероризму, наприклад, якою є рф[24]. Втручання у роботу глобальних інформаційних систем, які забезпечують обіг криптоактивів, завдає шкоди не лише приватним, а й публічним інтересам. Можливі атаки дають змогу зловмисникам акумулювати кошти, які можуть надалі бути використані для фінансування терористичної діяльності. Крім того, це завдає збитків інвесторам, які втрачають можливість наповнювати фінансовими ресурсами (податками тощо) економіку ЄС. На наше переконання, у цьому аспекті було б доцільним впровадження превентивних засобів щодо кібербезпеки, скажімо, у партнерстві з надавачами цифрових послуг, криптобіржами. Розвиток нових технологій викликає нові кіберзагрози, тому парадигма кібербезпеки в праві ЄС, як видається, має бути, з одного боку, сталою і чітко визначеною, а з другого – вона повинна

забезпечувати гнучкість в окремих сферах. Тобто при виникненні нових кіберзагроз впровадження нових заходів протидії їм має бути максимально оперативним і, за можливості, відбуватися без необхідності суттєвих законодавчих змін, а в рамках існуючого правового регулювання кібербезпеки.

Динаміка розвитку права ЄС, а також зміст наявних проєктів і стратегій свідчать про чітке усвідомлення наскрізної цифровізації приватних і публічних правовідносин, а також серйозності загроз, що випливають з цього. Щоправда, це не надто наблизило створення єдиної організаційно-правової системи кібербезпеки в ЄС, яка б поєднала у собі комплексне правове регулювання на рівні інтеграційного об'єднання, органи з відповідними повноваженнями та майданчики оперативної комунікації між державами – членами ЄС. Найбільш імовірними причинами цього видаються політичні перепони, пов'язані з розмежуванням компетенції між ЄС (як наднаціональним інтеграційним об'єднанням) та його державами-членами, а також відсутність комплексного бачення сутності кібербезпеки. Потреба у формуванні єдиної системи кібербезпеки в ЄС пов'язана не лише з певною неузгодженістю дій у рамках ЄС, а й зі складним і несистематизованим правовим регулюванням у межах національного права багатьох держав-членів. Так, у ФРН, Франції, Швеції та деяких інших державах відсутні спеціальні закони про кібербезпеку. У більшості випадків джерелами правового регулювання стають закони про інформацію, інформаційну безпеку та захист персональних даних. Звісно, вони охоплюють лише незначну частину правовідносин, пов'язаних із захистом від кіберзагроз різного рівня.

У цьому контексті вартим уваги є досвід України як держави, що не лише досягла надзвичайно високого рівня цифровізації, а й перманентно протидіє кіберзагрозам, які посягають як на приватні, так і публічні правовідносини. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. № 2163-VIII[25], оновлений у 2022 р., з урахуванням повномасштабного збройного вторгнення російської федерації в Україну, вирізняється концептуальними підходами. Він фактично закладає підвалини нової галузі права і стає фундаментом для подальшого правового регулювання більш вузьких аспектів кібербезпеки. При цьому, як видається, деякі інші законодавчі акти потребують узгодження з його положеннями, зокрема, Закон України «Про Національну програму інформатизації» від 1 грудня 2022 р. № 2807-IX[26] не містить згадки про кібербезпеку, а лише про кіберзахист. Примітно, що у Законі України «Про основні засади забезпечення кібербезпеки України» кіберзахист визначається як «сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем»[27]. Однак, на нашу думку, в контексті реалізації принципу правової визначеності у Законі України «Про Національну програму інформатизації»

слід уточнити, що поняття кіберзахисту розуміється саме в контексті положень Закону України «Про основні засади забезпечення кібербезпеки України», як це було зазначено в пояснювальній записці до проєкту Закону України «Про Національну програму інформатизації» від 1 листопада 2021 р. № 6241.

Законодавство України про кібербезпеку, зокрема Стратегія кібербезпеки України, а також план її реалізації, базуються на Стратегії кібербезпеки ЄС. Парадоксально, але воно виглядає більш структурованим і логічним, аніж у ЄС. Йдеться про комплексне бачення кібербезпеки та кіберзагроз. Зокрема, у ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» визначено, що кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання й нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі[28]. Українські науковці теж звертають увагу на те, що реалізація норм національного законодавства про кібербезпеку має бути скерована на забезпечення безпечного функціонування кіберпростору та його використання в інтересах людини, суспільства і держави[29]. Наведене свідчить про існування концепції кібербезпеки, відповідно до якої остання включає приватну та публічну складові. Перша стосується захисту прав та інтересів фізичних і юридичних осіб, а друга – питань оборони держави та захисту критичної інфраструктури. Водночас більшість держав – членів ЄС взагалі не розглядають кіберзахист як складовий компонент кібербезпеки[30].

Варто зазначити, що, незважаючи на те, що правове регулювання кібербезпеки України в деяких аспектах випередило право ЄС з об'єктивних причин (необхідність протидії російським кібератакам як елементу повномасштабного вторгнення), у контексті отримання Україною статусу кандидата на вступ до ЄС, ратифікації Угоди між Україною та Європейським Союзом про участь України у програмі Європейського Союзу «Цифрова Європа» (2021–2027)[31], яка має на меті, inter alia, налагодження взаємовигідного співробітництва з метою зміцнення та підтримки розгортання надійних і безпечних цифрових можливостей, серед іншого, у сфері кібербезпеки, вітчизняному законодавцю необхідно відстежувати зміни у правовому регулюванні кібербезпеки в рамках інтеграційного об'єднання та швидко реагувати на них.

Єдина система кібербезпеки ЄС потребує існування розвиненої інституційної основи, яка б гарантувала реалізацію прав та інтересів приватних суб'єктів, а також безпеку критичної інфраструктури ЄС і його держав-членів. Наявна диспозитивна модель інституційних гарантій спрямована на встановлення стандартизації (приватна складова кібербезпеки) або комунікацію та обмін досвідом (публічна складова кібербезпеки). Погоджуємося з позицією вчених Л. Мартіно і Н. Гамал про те, що неможливо (і небезпечно) копіювати рішення, які були дієвими для старих явищ, щоб керувати новою

динамікою кіберпростору[32]. ЄС доцільно визнати, що кібербезпека є окремою глобальною проблематикою, яка потребує спеціального правового регулювання та органів зі спеціальними повноваженнями.

Вважаємо, що багаторічний позитивний досвід роботи ENISA дає змогу розглянути можливість розширення повноважень цього органу. До структури цього агентства можуть увійти підрозділи із безпеки криптоактивів, підрозділи, наділені певними контролюючими повноваженнями, а також підрозділи, уповноважені реагувати на факти порушень з боку зобов'язаних суб'єктів. Можливість надання ENISA повноважень з питань кіберзахисту є не надто однозначною. У будь-якому випадку цей орган має бути задіяний до забезпечення публічної складової кібербезпеки, однак особливості такої складової вказують на необхідність утворення окремого спеціального органу. Вочевидь існуюча диспозитивна модель не дає змоги запровадити в межах ЄС спільну систему активного кіберзахисту, потреба в якій актуалізувалася після різних кібератак. Водночас такий спосіб протидії кіберзагрозам вперше було запроваджено у Законі України «Про основні засади забезпечення кібербезпеки України»[33] шляхом внесення до нього змін у 2022 р.[34]

Висновки. Отже, парадигма кібербезпеки у праві ЄС викристалізувалася на основі концепції «мережевої та інформаційної безпеки». Комплексного дослідження потребує питання, чи наразі кібербезпека має охоплювати не лише мережеву та інформаційну безпеку, а й, можливо, так звану криптобезпеку (безпеку у сфері криптовалют), яка поступово стає невід'ємним елементом користування ІКТ у сучасних реаліях. Примітно, що в актах ЄС робиться акцент на важливості кібербезпеки для забезпечення функціонування внутрішнього ринку ЄС, а не захисту прав людини. Проте, на нашу думку, не можна вважати виправданим бачення захисту прав людини, передусім основоположних прав, як другорядної складової кібербезпеки.

Право ЄС прямо не визначає дихотомію парадигми кібербезпеки, однак дає змогу виокремити її приватну та публічну складові. Приватна складова кібербезпеки зосереджена на захисті прав та інтересів окремих осіб і компаній від втручань у їхні соціальні, економічні та інші приватні відносини. При цьому публічна складова кібербезпеки фокусується на захисті від кіберзагроз, які загрожують національним інтересам держав – членів ЄС, інтересам самого інтеграційного об'єднання, а також критичній інфраструктурі. Окреслена подвійна природа кібербезпеки потребує релевантного законодавчого врегулювання, особливо з огляду на різні підходи та можливості держав-членів у забезпеченні кібербезпеки, що є ключовим для створення безпечного кіберпростору. У цьому контексті вартим уваги є досвід України як держави, що не лише досягла надзвичайно високого рівня цифровізації, а й перманентно протидіє кіберзагрозам. Водночас Україні варто переймати досвід правового регулювання кібербезпеки в ЄС, особливо у таких інноваційних сферах, як ринки криптовалют.

Серед можливих підходів до розуміння сутності кібербезпеки (включно у сфері використання криптоактивів) вважаємо за доцільне віддати перевагу широкому підходу. В такому випадку можливе формування права на кібербезпеку, яке включає не лише стан технічної захищеності, а й належні правові та інституційні гарантії захисту і відшкодування заподіяної шкоди. Однак формування ефективних механізмів відшкодування, особливо на ринках криптоактивів, вимагатиме багато часу в зв'язку зі складною правовою природою криптовалют і їхньою величезною кількістю.

Інституційні гарантії кібербезпеки засновані на роботі деяких важливих органів ЄС, найбільш вагоме місце серед яких посідає ENISA. Закріплення права на кібербезпеку, а також сучасні реалії цифровізації, зокрема впровадження блокчейн-технологій і криптовалют, вимагають трансформації структури та повноважень цього агентства. Окрім координаційних функцій, ENISA має отримати базові контрольні функції та механізми реагування на порушення права на кібербезпеку. Крім того, ця агенція має отримати низку повноважень, спрямованих на захист прав та інтересів користувачів криптоактивів. Обсяг їх використання свідчить про те, що вони поступово стають суттєвою складовою внутрішнього ринку ЄС.

Наостанок резюмуємо, що стрімкий розвиток ІКТ у цифрову епоху вимагає кіберобізнаності та надзвичайно швидкого реагування законодавця, а також виконання елементарних вимог з кібернетичної безпеки. У сучасних умовах цифровізації парадигма кібербезпеки у праві ЄС має бути водночас сталою (в загальних підходах) і гнучкою, зокрема, коли йдеться про правове регулювання її окремих складових.

1. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Single Market Strategy for Europe. COM/2015/0192 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192 **2.** 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). Official Journal of the European Union. L 151. 07.06.2019. P. 15–69. URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj **3.** Europol report. Cybercrime areas. Europol: website. URL: https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime **4.** Звоздецька О. Я. Кібербезпека ЄС в умовах посилення кіберзагроз в сучасному глобалізованому світі. Медіафорум: аналітика, прогнози, інформаційний менеджмент. 2019. Т. 7. С. 29. URL: http://nbuv.gov.ua/UJRN/mfapim_2019_7_4 **5.** Грубінко А. В. Особливості формування політики кібербезпеки Європейського Союзу: правові аспекти. *Актуальні проблеми правознавства.* 2021. Вип. 1. С. 6. URL: http://nbuv.gov.ua/UJRN/aprpr_2021_1_3 **6.** 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). Official Journal of the European Union. L 151. 07.06.2019. P. 15–69. URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj

7. Papakonstantinou V. Cybersecurity as Praxis and as a State: the EU Law Path Towards Acknowledgement of a New Right to Cybersecurity? Computer Law & Security Review. 2022. Vol. 44. P. 3. URL: https://www.sciencedirect.com/science/article/pii/S0267364922000012?via%3Dihub **8.** Cybersecurity. Cambridge Dictionary: website. URL: https://dictionary.cambridge.org/dictionary/english/cybersecurity **9.** Seemma P. S., Nandhini S., Sowmiya M. Overview of Cyber Security. *International Journal of Advanced Research in Computer and Communication Engineering.* 2018. Vol. 7. Issue 11. P. 125. URL: https://www.researchgate.net/publication/329678338_Overview_of_Cyber_Security **10.** Papakonstantinou V. Op. cit. P. 3 **11.** 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). Official Journal of the European Union. L 151. 07.06.2019. P. 15–69. URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj **12.** European Commission and the High Representative of the Union for Foreign Affairs and Security Policy. The EU's Cybersecurity Strategy for the Digital Decade, 2020. European Commission: website. URL: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 **13.** 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.* L 194. 19.07.2016. P. 1–30. URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj **14.** Consolidated version of the Treaty on European Union. Official Journal of the European Union. C 326. 26.10.2012. P. 13–390. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012M%2FTXT **15.** Mazurier P. A. Cybersecurity Landscape: Technological Perspectives and Certification Framework, Products, and Services. European Cybersecurity in Context A Policy-Oriented Comparative Analysis. 2022. P. 3. URL: https://liberalforum.eu/wp-content/uploads/2022/08/European-Cybersecurity-in-Context_ELF-Study_Techno-Politics.pdf **16.** Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance). *Official Journal of the European Union.* L 333. 27.12.2022. P. 1–79. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554 **17.** Today's Cryptocurrency Prices by Market Cap. Coinmarketcap: website. URL: https://coinmarketcap.com/ **18.** Chan T. The nature of property in cryptoassets. Legal studies. Published online by Cambridge University Press: 18 January 2023. URL: https://www.cambridge.org/core/journals/legal-studies/article/nature-of-property-in-cryptoassets/6B882C05BD3D9A7A924FBE41C359E92E **19.** See: Kerr D. S., Loveland K. A., Smith K. T., Smith, L. M. Cryptocurrency risks, fraud cases, and financial performance. *Risks.* 2023. Vol. 11. No. 51. P. 1–15. URL: https://www.mdpi.com/2227-9091/11/3/51 **20.** Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (Text with EEA relevance). Official Journal of the European Union. L 150. 09.06.2023. P. 40–205. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1114 **21.** European Supervisory Authorities (EBA, ESMA and EIOPA). EU financial regulators warn consumers on the risks of crypto-assets, 2022. ENISA: website. P. 2. URL: https://www.esma.europa.eu/sites/default/files/library/esa_2022_15_joint_esas_warning_on_crypto-assets.pdf **22.** See: European Union Agency for Cybersecurity. Crypto Assets: Introduction to Digital Currencies and Distributed Ledger Technologies. 2021. ENISA: website. URL: https://www.enisa.europa.eu/publications/crypto-assets-introduction-to-digital-currencies-and-distributed-ledger-technologies **23.** European Supervisory Authorities (EBA, ESMA and EIOPA). EU financial regulators warn consumers on the risks of crypto-assets, 2022. ENISA: website. P. 2. URL: https://www.esma.europa.eu/sites/default/files/library/esa_2022_15_joint_esas_warning_on_crypto-assets.pdf **24.** Joint motion for a resolution on recognising the Russian Federation as a state sponsor of terrorism. (2022-2896(RSP). European Parliament: website. URL: https://www.europarl.europa.eu/doceo/document/RC-9-2022-0482_EN.html **25.** Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text **26.** Про Національну програму інформатизації: Закон України від 1 грудня 2022 року № 2807-IX. URL: https://zakon.rada.gov.ua/laws/show/2807-20#Text **27.** Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text **28.** Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text **29.** «Цифрова Україна»: конституційно-правова модель / за ред. Р. О. Стефанчука, О. Л. Копиленка та ін. Київ: Інститут законодавства Верховної Ради України, 2021. С. 121. **30.** Bendiek A., Maat E.P. The EU's Regulatory Approach to Cybersecurity. Stiftung Wissenschaft und Politik, 2019. P. 21. URL: https://www.swp-berlin.org/publications/products/arbeitspapiere/WP_Bendiek_Pander_Maat_EU_Approach_Cybersecurity.pdf **31.** Угода між Україною та Європейським Союзом про участь України у програмі Європейського Союзу «Цифрова Європа» (2021–2027). URL: https://zakon.rada.gov.ua/laws/show/984_005-22#Text **32.** Martino L., Gamal N. Editorial: European Cybersecurity in Context. European Cybersecurity in Context A Policy-Oriented Comparative Analysis. 2022. P. VIII. URL: https://liberalforum.eu/wp-content/uploads/2022/08/European-Cybersecurity-in-Context_ELF-Study_Techno-Politics.pdf **33.** Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text **34.** Про внесення змін до деяких законів України щодо забезпечення формування та реалізації державної політики у сфері активної протидії агресії у кіберпросторі: Закон України від 28 липня 2022 року № 2470-IX. URL: https://zakon.rada.gov.ua/laws/show/2470-20#n21

References

1. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Single Market Strategy for Europe. COM/2015/0192 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192 **2.** 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). *Official Journal of the European Union.* L 151. 07.06.2019. P. 15–69. URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj **3.** Europol report. Cybercrime areas. Europol: website. URL: https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime **4.** Zvozdetska O. Ya. Kiberbezpeka YeS v umovakh posylennia kiberzahroz v suchasnomu hlobalizovanomu sviti. Mediaforum: analityka, prohnozy, informatsiinyi menedzhment. 2019. T. 7. S. 29. URL: http://nbuv.gov.ua/UJRN/mfapim_2019_7_4 **5.** Hrubinko A. V. Osoblyvosti formuvannia polityky kiberbezpeky Yevropeiskoho Soiuzu: pravovi aspekty. Aktualni

problemy pravoznavstva. 2021. Vyp. 1. S. 6. URL: http://nbuv.gov.ua/UJRN/aprpr_2021_1_3 **6.** 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). Official Journal of the European Union. L 151. 07.06.2019. P. 15–69. URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj **7.** Papakonstantinou V. Cybersecurity as Praxis and as a State: the EU Law Path Towards Acknowledgement of a New Right to Cybersecurity? Computer Law & Security Review. 2022. Vol. 44. P. 3. URL: https://www.sciencedirect.com/science/article/pii/S0267364922000012?via%3Dihub **8.** Cybersecurity. Cambridge Dictionary: website. URL: https://dictionary.cambridge.org/dictionary/english/cybersecurity **9.** Seemma P.S., Nandhini S., Sowmiya M. Overview of Cyber Security. *International Journal of Advanced Research in Computer and Communication Engineering.* 2018. Vol. 7. Issue 11. P. 125. URL: https://www.researchgate.net/publication/329678338_Overview_of_Cyber_Security **10.** Papakonstantinou V. Op. cit. P. 3 **11.** 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). Official Journal of the European Union. L 151. 07.06.2019. P. 15–69. URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj **12.** European Commission and the High Representative of the Union for Foreign Affairs and Security Policy. The EU's Cybersecurity Strategy for the Digital Decade, 2020. European Commission: website. URL: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 **13.** 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.* L 194. 19.07.2016. P. 1–30. URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj **14.** Consolidated version of the Treaty on European Union. Official Journal of the European Union. C 326. 26.10.2012. P. 13–390. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012M%2FTXT **15.** Mazurier P.A. Cybersecurity Landscape: Technological Perspectives and Certification Framework, Products, and Services. European Cybersecurity in Context A Policy-Oriented Comparative Analysis. 2022. P. 3. URL: https://liberalforum.eu/wp-content/uploads/2022/08/European-Cybersecurity-in-Context_ELF-Study_Techno-Politics.pdf **16.** Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance). Official Journal of the European Union. L 333. 27.12.2022. P. 1–79. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554 **17.** Today's Cryptocurrency Prices by Market Cap. Coinmarketcap: website. URL: https://coinmarketcap.com/ **18.** Chan T. The nature of property in cryptoassets. Legal studies. Published online by Cambridge University Press: 18 January 2023. URL: https://www.cambridge.org/core/journals/legal-studies/article/nature-of-property-in-cryptoassets/6B882C05BD3D9A7A924FBE41C359E92E **19.** See: Kerr D.S., Loveland K.A., Smith K.T., Smith, L.M. Cryptocurrency risks, fraud cases, and financial performance. Risks. 2023. Vol. 11. No. 51. P. 1-15. URL: https://www.mdpi.com/2227-9091/11/3/51 **20.** Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (Text with EEA relevance). Official Journal of the European Union. L 150. 09.06.2023. P. 40–205. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1114 **21.** European Supervisory Authorities (EBA, ESMA and EIOPA). EU financial regulators warn consumers on the risks of crypto-assets, 2022. ENISA: website. P. 2. URL: https://www.esma.europa.eu/sites/default/files/library/esa_2022_15_joint_esas_warning_on_crypto-assets.pdf **22.** See: European Union Agency for Cybersecurity. Crypto Assets: Introduction to Digital Currencies and Distributed Ledger Technologies. 2021. ENISA: website. URL: https://www.enisa.europa.eu/publications/crypto-assets-introduction-to-digital-currencies-and-distributed-ledger-technologies **23.** European Supervisory Authorities (EBA, ESMA and EIOPA). EU financial regulators warn consumers on the risks of crypto-assets, 2022. ENISA: website. P. 2. URL: https://www.esma.europa.eu/sites/default/files/library/esa_2022_15_joint_esas_warning_on_crypto-assets.pdf **24.** Joint motion for a resolution on recognising the Russian Federation as a state sponsor of terrorism. (2022-2896(RSP). European Parliament: website. URL: https://www.europarl.europa.eu/doceo/document/RC-9-2022-0482_EN.html **25.** Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 5 zhovtnia 2017 roku № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text **26.** Pro Natsionalnu prohramu informatyzatsii: Zakon Ukrainy vid 1 hrudnia 2022 roku № 2807-IX. URL: https://zakon.rada.gov.ua/laws/show/2807-20#Text **27.** Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 5 zhovtnia 2017 roku № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text **28.** Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 5 zhovtnia 2017 roku № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text **29.** «Tsyfrova Ukraina»: konstytutsiino-pravova model / za red.: R. O. Stefanchuka, O. L. Kopylenka. Kyiv: Instytut zakonodavstva Verkhovnoi Rady Ukrainy, 2021. S. 121. **30.** Bendiek A., Maat E.P. The EU's Regulatory Approach to Cybersecurity. Stiftung Wissenschaft und Politik, 2019. P. 21. URL: https://www.swp-berlin.org/publications/products/arbeitspapiere/WP_Bendiek_Pander_Maat_EU_Approach_Cybersecurity.pdf **31.** Uhoda mizh Ukrainoiu ta Yevropeiskym Soiuzom pro uchast Ukrainy u prohrami Yevropeiskoho Soiuzu «Tsyfrova Yevropa» (2021-2027). URL: https://zakon.rada.gov.ua/laws/show/984_005-22#Text **32.** Martino L., Gamal N. Editorial: European Cybersecurity in Context. European Cybersecurity in Context A Policy-Oriented Comparative Analysis. 2022. P. VIII. URL: https://liberalforum.eu/wp-content/uploads/2022/08/European-Cybersecurity-in-Context_ELF-Study_Techno-Politics.pdf **33.** Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 5 zhovtnia 2017 roku № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text **34.** Pro vnesennia zmin do deiakykh zakoniv Ukrainy shchodo zabezpechennia formuvannia ta realizatsii derzhavnoi polityky u sferi aktyvnoi protydii ahresii u kiberprostori: Zakon Ukrainy vid 28 lypnia 2022 roku № 2470-IX. URL: https://zakon.rada.gov.ua/laws/show/2470-20#n21

Falalieieva Liudmyla, Strilets Bohdan. **Paradigm of cybersecurity in European Union law: modern realities in the context of digitalisation**

The study analyses the current paradigm of cybersecurity in the law of the European Union in the context of digitalisation. The authors highlight the doctrinal approaches to the definition of cybersecurity within this integration association. They analyse the EU acts which emphasise the importance of cybersecurity for ensuring the functioning of the EU internal market rather than ensuring the observance of human rights, especially fundamental rights, which cannot be considered justified.

It is noted that EU law does not explicitly define the dichotomy of the cybersecurity paradigm, but it does allow for the distinction between its private and public components. The private component of cybersecurity is focused on protecting the rights and interests of individuals and companies from interference in their social, economic and other private relations. At the same time, the public component of cybersecurity focuses on protecting against cyber threats that threaten the national interests of EU Member States, the interests of the EU itself, and critical infrastructure. The outlined dual nature of cybersecurity requires adequate legislative regulation, especially given the different approaches and capabilities of Member States in ensuring cybersecurity. The authors believe that in this context, the experience of Ukraine, as a country that has not only achieved an extremely high level of digitalization but also constantly counteracts cyber threats, is worthy of attention. At the same time, Ukraine should adopt the experience of legal regulation of cybersecurity in the EU, especially in such innovative areas as cryptocurrency markets.

The authors prefer a broad approach to the definition of cybersecurity in EU law. In this case, it is possible to formulate the right to cybersecurity, which includes not only the state of technical security, but also appropriate legal and institutional guarantees of protection and compensation for damage. However, in this context, it is noted that the development of effective compensation mechanisms, especially in crypto-asset markets, will take a long time due to the complex legal nature of cryptocurrencies and their huge number.

It is concluded that the introducing the right to cybersecurity into EU law, as well as the current realities of digitalisation, require a transformation of the structure and powers of the European Union Agency for Cybersecurity (ENISA). In addition to coordination functions, ENISA should be given basic control functions and mechanisms for responding to violations of the right to cybersecurity. In addition, this agency should be granted a number of powers aimed at protecting the rights and interests of crypto-asset users. The extent of their use in the international economy shows that they are gradually becoming a significant component of the EU internal market.

Key words: *EU law, EU acts, EU citizens, cybersecurity, cyber defence, digitalisation, information and communication technologies, EU internal market, free movement of capital in the EU, European integration.*

DOI: 10.33663/0869-2491-2024-35-683-696
УДК 340.1

О. В. КРЕСІН,
*доктор юридичних наук, професор**
ORCID: 0000-0002-4016-6596

СУЧАСНА МОЗАЇКА ОСМИСЛЕННЯ КАРТИНИ СВІТУ В ПОРІВНЯЛЬНОМУ ПРАВОЗНАВСТВІ

У статті розглянуто теоретико-методологічні засади сучасних спроб осмислення картини світу права в порівняльному правознавстві. Основою таких пошуків є розрізнення, аналіз та порівняння домодерного, модерного та постмодерного правового розвитку та правового світогляду, які загалом співвідносяться з донаціональними, національними правовими порядками та кризою останніх. Зроблено висновок, що нові фрагментарні, але значною мірою узгоджені, бачення спеціальної картини світу порівняльного правознавства передбачають насамперед: деконструкцію національного та міжнародного права, піддаючи сумніву системність і тотальність першого та цілісність другого; і глобальний плюралізм правових порядків, режимів та їх елементів різного соціального та комунікативного походження. Утім, концептуально цілісна альтернатива націо- і державоцентричності у порівняльному правознавстві поки що не запропонована.

Ключові слова: *наукова картина світу, порівняльне правознавство, постмодернізм, правовий плюралізм, правовий порядок, національна правова система.*

Kresin Oleksiy. **Modern mosaic of understanding the picture of the world in comparative jurisprudence**

The article examines the theoretical and methodological foundations of modern attempts to understand the picture of the world of law in comparative jurisprudence. The basis of such searches is the distinction, analysis and comparison of pre-modern, modern and post-modern legal development and legal outlook, which are generally correlated with pre-national, national legal orders, and the crisis of the latter. The author comes to the conclusion that the new fragmentary, but largely agreed, visions of a special picture of the world of comparative jurisprudence providing for, first of all: the deconstruction of national and international law, questioning the systematicity and totality of the first and the integrity of the second; and the global pluralism of legal orders, regimes and their elements of various social and communicative origins. However, a conceptually coherent alternative to nation- and state-centricity in comparative jurisprudence has not yet been proposed.

Key words: *scientific picture of the world, comparative jurisprudence, comparative law, postmodernism, legal pluralism, legal order, national legal system.*

* ***Kresin Oleksii****, Doctor of Juridical Sciences, Full Professor*