МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет «Одеська юридична академія»

КАФЕДРА ЗАГАЛЬНОЇ ТЕОРІЇ ПРАВА ТА ДЕРЖАВИ

СИНТАГМИ СУЧАСНОЇ ЮРИСПРУДЕНЦІЇ : ПРОЛЕГОМЕНИ ПРАВОВОЇ ІННОВАТИКИ

до 80-річчя від дня народження

доктора юридичних наук, професора Юрія Миколайовича Оборотова

матеріали

всеукраїнської науково-практичної конференції

14 вересня 2026 року

Одеса

2026

УДК 340
DOI: https://doi.org/10.32837/11300.33882

Матеріали подано в авторській редакції

Синтагми сучасної юриспруденції : пролегомени правової інноватики. Пам’яті проф. Ю. М. Оборотова : (до 80-річчя від дня народж. д. ю. н., проф. Ю. М. Оборотова) : матер. Всеукр. наук.-практ. конф.(Одеса, 14 верес. 2026 р. Одеса : Нац. ун-т «Одеська юрид. академія»., 2026. 274 с. URL: https://doi.org/10.32837/11300.33882

Матеріали конференції, вміщені у цьому збірнику, відображають прагнення представників української правничої науки осмислити методологічне значення наукової спадщини Ю. М. Оборотова та розглянути актуальні проблеми розвитку сучасної юриспруденції. У працях авторів досліджуються питання методології юридичної науки, традиційні та інноваційні напрями розвитку права, трансформація держави, зміна правової реальності під впливом глобалізаційних, інтеграційних, інформаційних і технологічних процесів.

Окрему увагу приділено проблемам цифровізації права, ролі штучного інтелекту у трансформації юридичної діяльності, зміні форм правового регулювання, розвитку правової системи в умовах європейської інтеграції, а також переосмисленню фундаментальних категорій загальної теорії права та держави.

5. Лазовскі А. Верховенство права Європейського Союзу: юридична авантюра, що окупилася. *Право України*. 2019. № 6. С. 35–52. URL: https://pravoua.com.ua/storage/files/magazines/files/article-pravo_2019_6-s2.pdf

6. International Commission on Intervention and State Sovereignty. The Responsibility to Protect: Report of the International Commission on Intervention and State Sovereignty. Ottawa : *International Development Research Centre*, 2001. 91 p. URL: https://www.globalr2p.org/resources/the-responsibility-to-protect-report-of-the-international-commission-on-intervention-and-state-sovereignty-2001

Ключові слова: державний суверенітет, суверенна влада, міжнародно-правові зобов'язання, регіональна інтеграція, наднаціональні інституції, відповідальність захищати, державна незалежність, територіальна цілісність.

Key words: state sovereignty, sovereign power, international legal obligations, regional integration, supranational institutions, responsibility to protect, state independence, territorial integrity.

Тіхонов Анатолій Миколайович

Мелітопольський державний педагогічний університет імені Богдана Хмельницького здобувач вищої освіти спеціальності D8 «Право», експерт Національного агентства із забезпечення якості вищої освіти

Науковий керівник: **Устюжанінова Ольга Тарасівна**

Мелітопольський державний педагогічний університет імені Богдана Хмельницького кандидат юридичних наук, доцент кафедри права

DOI:

ПРАВОВІ МЕЖІ ДЕРЖАВНОГО ВТРУЧАННЯ У ФУНКЦІОНУВАННЯ КРИТИЧНИХ ЦИФРОВИХ МЕРЕЖ

Цифрова трансформація перетворила електронні комунікаційні мережі, дата-центри, точки обміну інтернет-трафіком і хмарні інфраструктури на основу функціонування держави, економіки та системи публічної безпеки. Порушення їх роботи має не лише техніко-економічний, а й безпековий характер.

Значна частина таких мереж перебуває у приватній власності. Це створює напругу між публічним інтересом у кіберстійкості та приватною автономією власників. Держава зобов'язана забезпечувати національну безпеку, проте ця функція не може виправдовувати необмежене втручання у право власності та свободу підприємництва. Конституція України одночасно закріплює безпекову функцію держави, верховенство права і гарантії власності [1].

Такий підхід відповідає загальній установці на розвиток юридичної науки через пошук нових способів осмислення права. Як наголошують представники Одеської школи права у колективній монографії за редакцією Ю. М. Оборотова, «необхідність творчого начала в дослідженнях права і держави робить креативність надзначущою рисою сучасної юриспруденції» [2, с. 3]. Для дослідження критичних цифрових мереж ця теза має безпосереднє методологічне значення, оскільки динамічний характер цифрових загроз потребує пошуку таких правових механізмів, які одночасно забезпечують безпеку та не допускають невиправданого розширення державного втручання.

Приватна власність не усуває публічної значущості цифрових мереж. Виведення з ладу системно важливого оператора може паралізувати банківський сектор, екстрені служби та органи влади. Тому статус оператора критичної цифрової інфраструктури слід розглядати як особливий правовий режим, за якого приватний суб'єкт зберігає власність, але набуває публічно-правових обов'язків.

Такі обов'язки пропоную визначати як квазіпублічні. Вони охоплюють: утримання від дій, що загрожують безперервності мережі; забезпечення кіберзахисту та резервування; співпрацю з державними органами під час кіберінцидентів. Закон України «Про критичну інфраструктуру» та Закон України «Про електронні комунікації» вже закріплюють відповідні вимоги [3; 4]. Водночас покладення таких обов'язків не має перетворюватися на перекладення всього тягаря безпеки на бізнес. Легітимність втручання визначається його необхідністю та співмірністю.

Людиноцентричний характер права вимагає, щоб державна та кібербезпека не розглядалися відокремлено від прав користувачів цифрових послуг. Як слушно наголошують представники Одеської школи права у

монографії «Креативність загальнотеоретичної юриспруденції» (за ред. Ю. М. Оборотова), «мірою всіх речей дійсно виступає благополуччя соціально-правового життя кожної конкретної людини і громадянина» [2, с. 18]. У контексті критичних цифрових мереж це означає, що забезпечення державної та кібербезпеки не може розглядатися відокремлено від прав та законних інтересів осіб, які користуються відповідними цифровими послугами.

Особливого значення цей підхід набуває у сфері доступу держави до цифрових комунікацій. У справі *Roman Zakharov v. Russia* Європейський суд з прав людини наголосив на необхідності достатніх правових гарантій проти свавільного втручання у приватне життя та комунікації, зокрема чіткого визначення підстав, процедур авторизації та контролю за відповідними заходами [7]. Отже, посилання на потреби безпеки не може саме по собі легітимізувати необмежений державний доступ до цифрових мереж.

Особливого правового значення проблема набуває в умовах воєнного стану. Збройна агресія зумовлює необхідність посилення державного управління критичною цифровою інфраструктурою, оскільки порушення електронних комунікацій може безпосередньо впливати на обороноздатність, функціонування органів влади та надання життєво важливих послуг. Закон України «Про правовий режим воєнного стану» передбачає можливість застосування спеціальних заходів щодо функціонування підприємств та інфраструктурних ресурсів в інтересах оборони і безпеки держави [5].

Практичним механізмом такого управління є Національний центр оперативно-технічного управління електронними комунікаційними мережами України (НЦУ). Відповідно до статті 32 Закону України «Про електронні комунікації», в умовах воєнного стану НЦУ здійснює оперативно-технічне управління мережами в межах наданих повноважень, взаємодіє з постачальниками та отримує інформацію про мережі і стан їх функціонування [4]. Розпорядження НЦУ щодо оперативно-технічного управління мережами в умовах воєнного стану є обов’язковими для виконання постачальниками.

Таким чином, воєнний стан створює конкретний механізм посиленого державного управління приватними електронними комунікаційними мережами. Водночас обов’язковість розпоряджень НЦУ не означає необмеженості

державної дискреції. На мою думку, саме за умов підвищеної інтенсивності втручання особливого значення набувають законність, визначеність компетенції, належне обґрунтування заходів та можливість їх правового контролю.

Отже, воєнний стан слід розглядати не як припинення дії принципу пропорційності, а як зміну допустимого рівня інтенсивності державного втручання. У мирний час пріоритетним є забезпечення приватної автономії за одночасного виконання оператором безпекових вимог. В умовах воєнного стану рівень державного управління може бути підвищений, але його межі визначаються законом, конкретною безпековою метою та необхідністю відповідного заходу.

Важливим орієнтиром для вдосконалення українського законодавства є Директива (ЄС) 2022/2555 (NIS 2), яка розмежовує суб'єктів на суттєві (*essential entities*) та важливі (*important entities*) і встановлює для них різну інтенсивність регуляторного нагляду [6]. Щодо суттєвих суб'єктів передбачено більш інтенсивний *ex ante* та *ex post* нагляд, тоді як щодо важливих переважає *ex post* підхід.

Цю модель необхідно відмежовувати від українського категорування об'єктів критичної інфраструктури за рівнями критичності. Я не вважаю доцільною механічну заміну національної системи категорування моделлю NIS 2. Натомість її окремі елементи можуть доповнити українське регулювання градуйованим режимом нагляду, за якого інтенсивність державного контролю залежатиме також від системного ризику, характеру діяльності оператора та потенційних наслідків порушення функціонування мережі.

Такий підхід відповідає принципу пропорційності: однакове регуляторне навантаження для суб'єктів із різним рівнем системного впливу може бути надмірним для одних і недостатнім для інших. Диференційований нагляд дозволяє концентрувати найбільш інтенсивні державні ресурси на суб'єктах, порушення діяльності яких здатне спричинити найбільш масштабні суспільні наслідки.

Кібернетичний вимір NIS 2 доцільно доповнювати підходом Директиви (ЄС) 2022/2557 (CER), яка орієнтується на загальну стійкість критичних

суб’єктів [8]. Її значення полягає в урахуванні не лише кіберризиків, а й природних, техногенних, фізичних та гібридних загроз. Для цифрових мереж це особливо актуально, оскільки їхня стійкість залежить також від електроживлення, резервних каналів, фізичного захисту обладнання та спроможності до відновлення.

На цій основі пропоную вдосконалення українського правового регулювання за трьома напрямами.

По-перше, доцільно нормативно закріпити принцип пропорційності державного втручання у функціонування критичної цифрової інфраструктури. Суб’єкт владних повноважень повинен обґрунтовувати легітимну мету, необхідність та співмірність відповідного заходу.

По-друге, необхідно розвивати градуйовану модель державного нагляду, яка враховуватиме існуюче українське категорування критичної інфраструктури та додатково оцінюватиме системний ризик оператора. Європейський поділ на *essential* та *important entities* може використовуватися як концептуальний орієнтир без механічного перенесення моделі NIS 2.

По-третє, необхідно посилити процедурні гарантії контролю за державним втручанням, особливо в умовах воєнного стану. Обов’язковість рішень та розпоряджень органів оперативного управління має супроводжуватися чітким визначенням їх компетенції, законних підстав, меж застосування та можливостей правового контролю.

Отже, правове регулювання критичних цифрових мереж повинно ґрунтуватися на узгодженні публічної безпеки та приватної автономії. Запропонована концепція квазіпублічних обов’язків поєднує приватну форму власності з особливою суспільною значущістю цифрової інфраструктури, принцип пропорційності визначає межі державного втручання, НЦУ демонструє механізм оперативного управління мережами в умовах воєнного стану, а моделі NIS 2 та CER створюють орієнтири для подальшого розвитку українського законодавства.

Наукова новизна запропонованого підходу полягає у розгляді правового режиму критичних цифрових мереж як системи взаємопов’язаних елементів: квазіпублічних обов’язків приватних операторів, пропорційності державного

втручання, градуйованого нагляду та спеціальних процедурних гарантій в умовах воєнного стану. На мою думку, така модель дозволяє протидіяти як надмірній державній концентрації контролю над цифровою сферою, так і недостатній відповідальності приватних операторів за стійкість критичної інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр (дата звернення: 01.09.2026).
2. Креативність загальнотеоретичної юриспруденції : монографія / [Ю. М. Оборотов, В. В. Завальнюк, В. В. Дудченко та ін.] ; за ред. Ю. М. Оборотова. Одеса : Фенікс, 2015. 488 с. URL: http://dspace.onua.edu.ua/handle/11300/3295 (дата звернення: 01.09.2026).
3. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 01.09.2026).
4. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20 (дата звернення: 01.09.2026).
5. Про правовий режим воєнного стану : Закон України від 12.05.2015 № 389-VIII. URL: https://zakon.rada.gov.ua/laws/show/389-19 (дата звернення: 01.09.2026).
6. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). Official Journal of the European Union. 2022. L 333. P. 80–152. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj
7. Case of Roman Zakharov v. Russia : Judgment of the European Court of Human Rights, Grand Chamber, 4 December 2015, application no. 47143/06. URL: https://hudoc.echr.coe.int/eng?i=001-159324

8. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities. Official Journal of the European Union. 2022. L 333. P. 164–198. URL: https://eur-lex.europa.eu/eli/dir/2022/2557/oj

Ключові слова: критичні цифрові мережі, правові межі, державне втручання, пропорційність, квазіпублічні обов'язки, кіберстійкість, воєнний стан.

Key words: critical digital networks, legal boundaries, state intervention, proportionality, quasi-public obligations, cyber resilience, martial law.