

УДК 340.01

ГРИЩЕНКО С.М., начальник підрозділу Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України
ORCID: <https://orcid.org/0000-0002-5922-280X>

ПРАВОВЕ РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ СУСПІЛЬСТВА

DOI: [https://doi.org/10.37750/2616-6798.2025.3\(54\).340519](https://doi.org/10.37750/2616-6798.2025.3(54).340519)

Анотація. У статті аналізується стан правового регулювання кібербезпеки в Україні в контексті цифрової трансформації сучасного суспільства. Проаналізовано вітчизняні здобутки в сфері цифровізації, а також інституціональні зміни у цій сфері. Розглянуто ключові проблеми нормативно-правового забезпечення захисту інформаційних систем, визначено недоліки чинного законодавства у сфері забезпечення кібербезпеки в Україні, запропоновано шляхи їх усунення, а також визначено перспективи правового забезпечення кібербезпеки в контексті цифрової трансформації суспільства. Особлива увага приділена європейським стандартам, які можуть бути впроваджені в національне законодавство для підвищення ефективності протидії кіберзагрозам.

Ключові слова: кібербезпека, цифрова трансформація, правове регулювання, національна безпека, інформаційні технології, кіберзагрози.

Summary. The article analyzes the state of legal regulation of cybersecurity in Ukraine in the context of the digital transformation of modern society. Domestic achievements in the field of digitalization, as well as institutional changes in this area, are analyzed. The key problems of regulatory and legal support for the protection of information systems are considered, the shortcomings of the current legislation in the field of cybersecurity in Ukraine are identified, ways to overcome them are proposed, and the prospects for legal support for cybersecurity in the context of the digital economy are also identified. Particular attention is paid to European standards and best practices that can be implemented in national legislation to increase the effectiveness of countering cyber threats.

Keywords: cybersecurity, digital transformation, legal regulation, national security, information technologies, cyber threats.

Постановка проблеми.

В умовах глобальної цифрової трансформації суспільства правове забезпечення кібербезпеки набуває особливого значення. Швидко змінюваний цифровий світ потребує формування більш збалансованої та ефективної національної системи забезпечення кібербезпеки, яка зможе гнучко адаптуватися до змін безпекового середовища, гарантуючи громадянам України безпечне функціонування національного сегмента кіберпростору, передбачивши нові можливості для цифровізації всіх сфер суспільного життя [1]. Зростання кількості кібератак, розвиток хмарних технологій, Інтернету речей (ІоТ), штучного інтелекту та інших новітніх напрямів цифровізації вимагають не лише технічних, але й комплексних правових рішень, спрямованих на ефективне реагування на нові кіберзагрози. Стратегія кібербезпеки України проголошує: “Україна має бути здатною забезпечити свій соціально-економічний розвиток у цифровому світі, що вимагає набуття спроможності ефективно стримувати деструктивні

дії в кіберпросторі, досягнення кіберстійкості на всіх рівнях та взаємодії всіх суб'єктів забезпечення кібербезпеки, яка ґрунтується на довірі” [1]. Ураховуючи виклики та загрози, що постали перед Україною у кіберпросторі, критично зростає роль кібербезпеки в процесах цифрової трансформації держави. Це зумовлює потребу вдосконалення правового забезпечення кібербезпеки України з урахуванням попереднього законодавчого досвіду, стану кібербезпекового середовища на національному та міжнародному рівні, а також визнаних міжнародних та європейських стандартів у цій сфері.

Результати аналізу наукових публікацій.

Правове забезпечення кібербезпеки в умовах цифрової трансформації є предметом поглибленої уваги науковців, серед як відзначимо напрацювання П.Войтович [2], П.Горіна [3], Д.Журбинського [4], Є.Колосовського [5], В.Костенко [4], С. Краснікова [6], С.Лучик [7], Н.Левицької [8], В.Луценко [9], Т.Пікулі, В.Сілаєва [3], І. Шопіної [10] та ін.

У 2022 р. видано навчальний посібник, в якому висвітлено правові засади забезпечення кібербезпеки в умовах цифрової трансформації, особливості та відмінності правового забезпечення кібернетичної безпеки України в цих умовах [11].

Метою статті є аналіз правового регулювання кібербезпеки в умовах цифрової трансформації суспільства для удосконалення концептуальних правових засад забезпечення кібербезпеки України.

Виклад основного матеріалу.

Перш ніж перейти до аналізу сучасного стану правового регулювання кібербезпеки в Україні, варто зупинитися на розумінні термінів “кібербезпека” та “цифрова трансформація”, які є ключовими для висвітлення предмета цієї статі.

Відповідно до положень ст. 1 Закону України “Про основні засади забезпечення кібербезпеки України” під терміном “кібербезпека” слід розуміти 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 і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [12].

Схоже визначення цього терміну міститься у Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2030 року, де кібербезпека розуміється як стан захищеності даних в електронному вигляді від їх несанкціонованого використання або кримінальних дій з цими даними, а також набір заходів для досягнення такого стану захищеності даних [13].

Щодо змісту терміну “кібербезпека” у юридичній літературі тривають дискусії.

В. Фурашев пояснює поняття “кібербезпеки” як стан здібностей людини, народу та держави загалом, стосовно запобігання та усунення, свідомого, прямого негативного впливу інформації [14, с. 164].

Схожої точки зору дотримується Д. Ширяєв, який відзначає: “кібербезпека є складною та багатогранною проблемою, яка вимагає спільних і постійних зусиль усіх зацікавлених сторін. Працюючи разом над розробкою найкращих практик, обміном інформацією та інвестуванням у нові технології, ми зможемо краще захистити себе та свою цифрову інфраструктуру від кіберзагроз” [15, с. 602].

О. Баранов під кібербезпекою пропонував розуміти інформаційну безпеку в умовах використання комп'ютерних систем та/або телекомунікаційних мереж [16, с. 61].

З наведених визначень випливають наступні ознаки кібербезпеки, які її характеризують як: 1) різновид інформаційної безпеки; 2) діяльність із забезпечення заінтересованими суб'єктами її захисту від несанкціонованого доступу до конфіденційної інформації, інших протиправних дій; 3) комплекс заходів, спрямованих на захист комп'ютерних систем та/або телекомунікаційних мереж, виявлення, запобігання негативного впливу інформації, інших загроз, пов'язаних з кіберпростором.

Для визначення поняття “цифрова трансформація” доцільно виділити його основу, зміст якої складає цифровізація.

Енциклопедія інформаційних наук і технологій містить таке визначення цифровізації – це “інтеграція цифрових технологій у повсякденне життя суспільства шляхом оцифровки всього, що можна оцифрувати. Цифровізація означає комп'ютеризацію систем і робочих місць для більшої легкості та доступності” [17].

У юридичній літературі розрізняють цифровізацію у вузькому і широкому розумінні.

Під цифровізацією у вузькому сенсі розуміють перетворення інформації в цифрову форму, яке у більшості випадків призводить до зниження видатків, та появи нових можливостей тощо[18, с.8].

Цифровізацію у широкому сенсі можливо розглядати як тренд ефективного світового розвитку тільки в тому випадку, якщо цифрова трансформація відповідає наступним вимогам: вона охоплює виробництво, бізнес, науку, соціальну сферу та звичайне життя громадян; супроводжується тільки ефективним використанням її результатів; її результати доступні користувачам перетвореної інформації; її результатами користуються не тільки фахівці, але й пересічні громадяни, а користувачі цифрової інформації мають навички роботи з нею[18, с.8].

Що стосується самого терміну “цифрова трансформація”, то під ним пропонується розуміти глибокий процес зміни всіх аспектів життя суспільства, зумовлений розвитком інформаційно-комунікаційних технологій шляхом перегляду бізнес-стратегії або цифрової стратегії, моделей, операцій, продуктів, маркетингового підходу, цілей тощо [19].

На думку І.Шопіної, під цифровою трансформацією слід розуміти оптимізацію організації, управління, функцій та методів діяльності, інформаційної культури та інформаційної свідомості суб'єктів правовідносин за рахунок використання ними інформаційних технологій [10, с. 32].

Як справедливо зазначає М.Хаустова, основною метою цифровізації є досягнення цифрової трансформації сфер життєдіяльності у нові більш ефективні та сучасні [18, с.8]. З її точки зору, цифровізація більш загальне поняття, яке охоплює багато методик, а цифрова трансформація – це процес, завдяки якому організації з використанням цифрових технологій переходять на новий рівень не тільки виробництва, а й відношення між партнерами, клієнтами та працівниками[18, с.9].

Отже, цифрова трансформація — це одночасно технологічна та культурна зміна, яка означає, що цифрові інструменти за своєю суттю забезпечують нові види інновацій та творчість в певній області, а не просто вдосконалюють та підтримують традиційні методи обробки інформації. Цифровізація, у свою чергу, призводить до появи нових об'єктів правовідносин, таких як цифрові речі [20].

Сучасна цифрова трансформація охоплює:

- цифрові платформи та онлайн-сервіси;
- штучний інтелект та машинне навчання;
- Інтернет речей (IoT);

блокчейн-технології;
хмарні обчислення;
нові технологій, цифрові послуги.

Все це в контексті сталого розвитку економіки та суспільства може сприяти досягненню Глобальних Цілей Сталого Розвитку Організації Об'єднаних Націй до 2030 року.

Основною метою державної політики в умовах цифрової трансформації є управління існуючими і можливими викликами та загрозами інформаційної безпеки з метою створення необхідних умов для функціонування інформаційного суспільства, вільного та безпечного кіберпростору, реалізації інформаційних прав людини та громадянина, цифрової трансформації держави та суспільства, захисту національних інтересів України у безпековій сфері [3, с.86]. Така мета знаходить відображення в Стратегії кібербезпеки України. Так, ціль К.3. “Безпечні цифрові послуги” Стратегії кібербезпеки звучить так: “Україна забезпечить досягнення балансу між потребами суспільства, вітчизняного ринку, економіки держави та необхідними заходами з кібербезпеки, а також надійності та безпеку цифрових послуг протягом усього їхнього життєвого циклу” [1]. Для досягнення цілі К.3 Україна спрямує зусилля на забезпечення надійності та безпеки цифрових послуг шляхом: зміцнення довіри приватного сектору та громадян до цифрових послуг, які надаються державою, безумовного виконання вимог щодо забезпечення кібербезпеки та кіберзахисту під час їх надання та інформування громадськості про їх безпечність та надійність; впровадження цифрових послуг для населення та розвитку національної інформаційної інфраструктури; розроблення національних стандартів у сфері кібербезпеки, організаційних та технічних вимог, що стосуються безпеки застосунків, мобільних пристроїв, робочих станцій, серверів і мереж, моделей хмарних обчислень, з урахуванням європейських та міжнародних стандартів; створення органів з оцінки відповідності надавачів електронних довірчих послуг вимогам для кваліфікованих надавачів кваліфікованих електронних довірчих послуг; створення необхідних передумов (нормативних, організаційних, технологічних) для автентифікації користувачів сервісів цифрових послуг (там, де це потрібно) за допомогою інтегрованої системи електронної ідентифікації з використанням технологій електронної ідентифікації та/або електронних довірчих послуг; підвищення ефективності системи захисту персональних даних громадян шляхом гармонізації законодавства України з відповідним законодавством ЄС та посилення відповідальності за порушення встановлених вимог [1].

Сьогодні не можна не відзначити часткову реалізацію цієї мети та певний прогрес розвитку цифрової трансформації процесів взаємодії громадянина і держави, а також діяльності органів державної влади. Урядом України останнім часом вживаються масштабні заходи з розвитку цифровізації суспільства, цифрового сектору економіки та вдосконалення нормативно-правової бази в сфері електронної демократії. Розпорядженням Кабінету Міністрів України від 12 червня 2019 року № 405-р затверджено План заходів щодо реалізації Концепції розвитку електронної демократії в Україні на 2019–2020 рр. Для реалізації цих та інших проектів 18 вересня 2019 року Уряд затвердив Положення про Міністерство цифрової трансформації України. У березні 2021 року Кабінет Міністрів України схвалив Концепцію розвитку цифрових компетентностей та затвердив план заходів з її реалізації, одним із яких є розроблення та затвердження опису цифрової компетентності (рамки цифрової компетентності) та відповідних рамок цифрових компетентностей для основних професійних груп за сферами економічної діяльності [18, с.10]. З 14.08.2021 р. набув чинності Закон України

“Про стимулювання розвитку цифрової економіки в Україні”, визначає організаційні, правові та фінансові засади функціонування правового режиму Дія Сіті, що запроваджується з метою стимулювання розвитку цифрової економіки в Україні шляхом створення сприятливих умов для ведення інноваційного бізнесу, розбудови цифрової інфраструктури, залучення інвестицій, а також талановитих спеціалістів.

Цифровізація публічних послуг суттєво підвищила їх якість. Незважаючи на певні недоліки системи “Дія”, а також єдиних і державних реєстрів (переважно пов’язаних із їх вразливістю до витоків персональних та інших даних), можна констатувати, що Україна вийшла на одне з перших місць в Європі у сфері цифрової трансформації органів публічного адміністрування. Єдина судова інформаційно-телекомунікаційна система, яка включає у тому числі й підсистему “Електронний суд”, дозволила зробити великий крок уперед на шляху підвищення доступності [3, с.84]. Пропонується повне впровадження електронного судочинства та інтеграція з українським мобільним застосунком “Дія”, який надає громадянам доступ до різноманітних цифрових послуг, що сприятиме зручності взаємодії із судовою системою. До цього переліку об’єктів цифровізації слід додати нові цифрові продукти, які були створені в час воєнного стану, а саме, “Армія+”, “Резерв+”.

І хоча упровадження нових технологій, цифрових послуг та механізмів електронної взаємодії громадян з державою, здійснюється безсистемно та без належної оцінки ризиків, станом на вересень 2024 року Україна посіла п’яте місце у світі за рівнем розвитку цифрових державних послуг та увійшла у топ-25 рейтингу країн світу за рівнем кібербезпеки. Це рейтинг ґрунтується на глобальному індексі, який оцінює рівень електронного урядування та залученість громадян до взаємодії з державою через електронні сервіси, а також вимірює готовність країн запобігати кіберзагрозам і відповідати на інциденти[21].

З одного боку, цифрова трансформація суспільства є важливим механізмом взаємодії громадян, бізнесу та держави. З іншого боку – сучасні цифрові інструменти – електронне урядування, цифрові банківські послуги, онлайн-освіта, цифрова медицина — все це розширює спектр потенційних кіберзагроз.

Сьогодні серед найбільш поширених потенційних загроз кібербезпеці можна виокремити:

- кібертероризм, кібердиверсію;
- dezінформаційні кампанії;
- порушення конфіденційності персональних даних;
- атаки типу DDoS;
- використання AI для проведення фішингових атак;
- несанкціонований доступ та інші вторгнення до державних інформаційних систем;
- маніпуляції з даними у хмарних сервісах.

Неабиякі труднощі для забезпечення цифрового процесу трансформації країни спричиняють гібридні військові дії, що тривають у світі та несуть ризики для системи електронних засобів і відповідних інформаційних продуктів, так як в світі “зараз триває перша кібервійна”, активні дії якої проходять на території різних державних та в різних формах прояву[3, с.84].

Але головною загрозою для державної безпеки України залишається агресія рф, у т.ч. у кіберпросторі. Слід погодитися з висновком П. Горіна та В. Сілаєва про те, що сьогодні існує потреба прийняття політичних рішень та нормативно-правового забезпечення у сфері цифрової трансформації як способу протидії інформаційним загрозам в умовах воєнної агресії російської федерації[3, с.86]. Слід також взяти до

уваги, що правове регулювання забезпечення кібербезпеки часто відстає від темпів технологічних змін, що створює правову невизначеність та ризики для національної безпеки. Саме тому Україна активно працює над подоланням інформаційного дисбалансу як в законотворчій сфері, так і в практичній площині діяльності відповідних суб'єктів [3, с.84].

За останні десять років в Україні сформовано потужну правову основу у сфері забезпечення кібербезпеки України, зміст якої складає: Конституція України, закони України “Про національну безпеку”, “Про захист інформації в автоматизованих системах”, “Про критичну інфраструктуру”, “Про основи забезпечення кібербезпеки України”, інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України.

Найбільш важливими є укази Глави держави про затвердження: Стратегії національної безпеки України, Стратегії забезпечення державної безпеки, Стратегії кібербезпеки України, а також Стратегії інформаційної безпеки.

Суттєві зміни щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури внесено Законом України від 27 березня 2025 року, який передбачає: створення та забезпечення функціонування національних систем реагування на інциденти кібербезпеки, кібератаки, кіберзагрози та обміну інформацією про інциденти кібербезпеки щодо інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем; правові засади для управління ризиками ланцюгу постачання шляхом запровадження постачальниками вимог безпеки відповідно до рівня ризику; законодавчі основи для побудови комплексних систем захисту інформації шляхом усунення бар'єрів для імплементації більш гнучкого порядку підтвердження відповідності; створення правових засад для запровадження системи оцінювання стану кіберзахисту; залучення Міністерства цифрової трансформації України, Міністерства закордонних справ України до складу основних суб'єктів національної системи кібербезпеки з визначенням їх основних завдань у вказаній сфері[22].

Однак нинішня система нормативно-правового забезпечення кібербезпеки характеризується фрагментарністю і залишається недосконалою, оскільки деякі нормативні приписи є декларативними, а частина – не реалізованими, що ускладнює їх застосування на практиці та обмежує ефективність такої системи. Надзвичайно важливі для розвитку національної системи кібербезпеки та цифровізації суспільства завдання Стратегії кібербезпеки України, не були виконані, зокрема: не розроблено Загальнонаціональної програми кіберграмотності, спрямованої на підвищення рівня цифрової грамотності населення України. Не повною мірою впроваджено інноваційні методики обробки та оцінки цифрових даних, формування електронних доказів для удосконалення аналітичного і криміналістичного забезпечення контррозвідувального захисту кібербезпеки держави.

Не дивлячись на значні зусилля, спрямовані на правове забезпечення кібербезпеки України, залишаються актуальними для України проголошені Стратегією забезпечення кібербезпеки виклики:

упровадження нових технологій, цифрових послуг та механізмів електронної взаємодії громадян з державою, що здійснюється безсистемно в частині заходів з кібербезпеки та без належної оцінки ризиків.

відсутність у значної частини державних органів необхідного кадрового забезпечення у частині їх комплектування досвідченими фахівцями з питань кібербезпеки;

неефективні механізми стимулювання фахівців з питань кібербезпеки та кіберзахисту до роботи в державному секторі;

незавершеність заходів з упровадження організаційно-технічної моделі кіберзахисту, яка відповідатиме сучасним загрозам, викликам у кіберпросторі та глобальним тенденціям розвитку індустрії кібербезпеки;

відсутність належної системи підвищення цифрової грамотності громадян та культури безпекового поведіння в кіберпросторі, низький рівень обізнаності суспільства щодо кіберзагроз та кіберзахисту;

недосконалість нормативно-правової бази у сфері кібербезпеки, повільна імплементація положень європейського законодавства, недостатня врегульованість цифрової складової розслідування кримінальних правопорушень, а також низький рівень правової відповідальності за порушення вимог законодавства у цій сфері[1].

Останнє зумовлює потребу завершення імплементації в національне законодавство приписів Конвенції ООН про кіберзлочинність 2001 року особливо в частині визначення кіберзлочинів, їх видів, надання міжнародної правової допомоги з їх розслідування.

Вельми важливим напрямком державної політики є оновлення Стратегії кібербезпеки України з урахуванням попереднього досвіду в умовах воєнного стану, положень Стратегії кібербезпеки ЄС на цифрове десятиліття, інших актів ЄС, а також стратегій кібербезпеки окремих держав-членів ЄС та держав-членів НАТО.

З огляду на прагнення України до вступу в ЄС надзвичайно актуальним з точки зору формування комплексного правового регулювання кібербезпеки залишається імплементація в національне законодавство відповідних правових актів ЄС, серед яких найбільш важливими є: Директива 2016/1148 про безпеку мережевих та інформаційних систем (NIS Directive), Директива 2022/2555 про мережеву та інформаційну безпеку (NIS 2 Directive), Стратегія кібероборони 2022 (EU Cyber Defence Policy Framework), Закон ЄС про кіберстійкість 2022 (The Cyber Resilience Act).

Реалізація цих правових актів ЄС: забезпечує високий рівень захисту персональних даних; передбачає законодавче забезпечення покращення стану кібербезпеки за допомогою удосконалення відповідних стандартів; гарантує право на конфіденційність та розширює межі міжнародної співпраці у сфері забезпечення кібербезпеки.

Ці акти передбачають створення на теренах ЄС нової європейської кібер-екосистеми, яка буде більш безпечною для усіх громадян незалежно від того, наскільки вони освічені у питаннях цифрової безпеки[23]. Саме вони визначають певні орієнтири для вдосконалення національного законодавства у сфері забезпечення кібербезпеки.

Висновки. Цифрова трансформація суспільства суттєво впливає на сферу кібербезпеки, яка вимагає адекватного правового забезпечення. Правове регулювання кібербезпеки в умовах цифрової трансформації суспільства має бути проактивним та довгостроковим, орієнтованим на прогнозування та запобігання новим видам кіберзагроз. Україна має потенціал для формування ефективної правової моделі кібербезпеки, однак це потребує системного підходу, модернізації законодавства, міжнародної інтеграції та посилення інституційного забезпечення[1].

Актуальним в умовах цифрової трансформації суспільства є удосконалення правового забезпечення кібербезпеки, спрямованого на захист інформаційних ресурсів, конфіденційність даних та забезпечення інформаційної безпеки. Одними з можливих

напрямків удосконалення такого забезпечення є: 1) посилення спроможностей з кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури; 2) введення обов'язкової сертифікації систем кібербезпеки для об'єктів критичної інфраструктури; 3) розвиток правового регулювання використання штучного інтелекту в сфері забезпечення кібербезпеки; 4) формування ефективного механізму реагування на кіберінциденти в кіберпросторі; 5) розвиток кадрового потенціалу та інноваційного ринку кібербезпеки, що сприятиме створенню національних розробок на рівні кращих світових практик для забезпечення можливості протидіяти майбутнім кіберзагрозам; 6) поліпшення взаємодії суб'єктів забезпечення кібербезпеки під час виявлення та запобігання кіберінцидентів; 7) активізація міжнародного співробітництва у сфері цифрової трансформації суспільства; 8) імплементація в національне законодавство приписів Конвенції ООН про кіберзлочинність для удосконалення законодавства про кримінальну відповідальність за кіберзлочини; 9) створення національних розробок на рівні кращих світових практик для забезпечення можливості протидіяти майбутнім кіберзагрозам; 10) підвищення рівня цифрової грамотності населення та культури безпекового поведіння в кіберпросторі. До виконання завдань із розвитку наукового потенціалу та поширення кіберграмотності слід активно залучати заклади освіти та наукові установи.

Реалізація запропонованих заходів сприятиме забезпеченню правового захисту суспільства, економіки та національної безпеки в умовах цифрової епохи, модернізації правового регулювання кібербезпеки в Україні та її інтеграції в європейський правовий простір. Цифрова трансформація є ключовим аспектом реформ державної влади. Це передбачає подальшу цифровізацію публічних функцій держави, що сприяє взаємозв'язку національних баз і реєстрів, а також забезпечення електронних каналів зв'язку між компетентними органами держави.

Використана література

1. Стратегія кібербезпеки України: затвердж. Указом Президента України від 26 серпня 2021 р. № 447. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text>.
2. Войтович П. Становлення організаційно-правового механізму захисту інформаційних прав людини. *Наукові праці Міжрегіональної академії управління персоналом*. 2024. Вип. 2. С. 32–37.
3. Сіласєв В., Горінов П. Політика інформаційної безпеки в умовах цифрової трансформації України: виклики та шляхи попередження *Наукові праці Міжрегіональної академії управління персоналом. Політичні науки та публічне управління* 2024. Випуск 3 (75). С. 81–87.
4. Журбинський Д. А., Костенко В.О. Актуальність посилення кібербезпеки України в умовах дії воєнного стану в контексті європейської інтеграції. *Публічне управління та адміністрування в Україні*. 2023. Випуск 34. С. 74–77.
5. Колосовський Є.Ю., Круць Е.М. Сучасний стан кібербезпеки України в умовах воєнного періоду. *Юридичний науковий електронний журнал*. 2023. №12. С. 403–405. URL: http://lsej.org.ua/12_2023/100.pdf.
6. Красніков С.А. Шляхи посилення стану забезпечення кібербезпеки в умовах воєнного стану. *Інформація і право*. 2023. № 3(46) С.118–128. URL: <http://il.ippi.org.ua/issue/view/17050>.
7. Лучик С.Д., Лучик В.Є. Кібербезпека в умовах війни: соціальні аспекти *Наука і техніка сьогодні*. 2024. № 7(35). С. 857–870.
8. Левицька Н.О. Сучасні тенденції розвитку нормативно-правового регулювання цифрової економіки. *Юридичний науковий електронний журнал*. 2019. №5. С. 26–29.

9. Луценко В.Р., Пікулі Т.О. Правове забезпечення цифрової трансформації в Україні. *Науковий вісник Ужгородського Національного Університету*, Серія ПРАВО. 2024. Випуск 81: частина 1. С. 61-67. URL:<http://visnyk-pravo.uzhnu.edu.ua/article/view/300456/292764>.
10. Шопіна І.М. Принципи цифрової трансформації України крізь призму досвіду Європейського Союзу. *Південноукраїнський правничий часопис*. 2022. № 4, ч. 3. С. 29–34.
11. Довгань О., Ткачук Н., Ткачук Т., Петров В. Правові засади забезпечення кібербезпеки в умовах цифрової трансформації. Навч. посіб. К., Артек. 2022. 171 с.
12. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.
13. Стратегія здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2030 року: схвалено розпорядженням Кабінету Міністрів України від 17 листопада 2021 р. № 1467. URL:<https://zakon.rada.gov.ua/laws/show/1467-2021-%D1%80#n15>.
14. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право*. 2012. № 2. С.162–169.
15. Ширяєв Д.О. Кібербезпека та сучасний світ. Актуальні проблеми сучасної науки в дослідженнях молодих учених, курсантів та студентів. Вінниця, 2023. С. 600–602.
16. Баранов О.А. Про тлумачення та визначення поняття “кібербезпека”. *Правова інформатика*. 2014. № 2(42). С. 54-62. URL:<https://ippi.org.ua/sites/default/files/14boavpk.pdf>
17. Encyclopedia of Information Science and Technology, Fourth Edition (10 Volumes). IGI Global, June. 2017. 8104 p.
18. Хаустова М.Г. Правове забезпечення цифрової трансформації у сучасних умовах. *Право та інновації*. 2022. № 2 (38). С. 7-18. URL:<https://openarchive.nure.ua/server/api/core/bitstreams/2cf09751-22a8-4b1e-b4ad-05ac036d49f3/content>.
19. Цифрова трансформація. URL:<https://uk.wikipedia.org/wiki>.
20. Правове регулювання цифрової трансформації й цифровізації у цивільному праві України URL:<https://law.chnu.edu.ua/pravove-rehuliuvannia-tsyfrovoi-transformatsii-y-tsyfrovizatsii-u-tsyvilnomu-pravi/>
21. Україна стала п'ятою у світі за рівнем розвитку цифрових держпослуг. URL: <https://forbes.ua/news/ukraina-stala-pyatoyu-u-sviti-za-rivnem-rozvitku-tsifrovikh-derzhposlug-20092024-23743>.
22. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури: Закон України від 27 березня 2025 р. № 4336-IX. URL: <https://zakon.rada.gov.ua/laws/show/4336-20#Text>.
23. Федієнко О.П. Європейський досвід законодавчого забезпечення посилення кіберстійкості. *Інформація і право*. 2024. № 2(49). С. 178-189.

~~~~~ \* \* \* ~~~~~