

О. О. Карапетянздобувач кафедри конституційного та адміністративного права
Запорізького національного університету

АДМІНІСТРАТИВНО-ПРАВОВІ ВИКЛИКИ ЗАБЕЗПЕЧЕННЯ СВОБОДИ СЛОВА В ЦИФРОВУ ЕПОХУ

У статті досліджуються сучасні адміністративно-правові виклики, що постають перед Україною у процесі забезпечення свободи слова в умовах цифровізації медіапростору. Акцентовується увага на трансформації традиційних механізмів державного регулювання інформаційної сфери, спричиненій розвитком цифрових технологій, розширенням функціоналу соціальних медіа, появою генеративного штучного інтелекту, а також загостренням проблем безпеки внаслідок збройної агресії Російської Федерації проти України.

В межах наукового дослідження проаналізовано відсутність комплексного нормативно-правового регулювання свободи слова в інтернет-просторі, що призводить до непослідовності правозастосовної практики та правової невизначеності статусу цифрових платформ, блогерів, адміністраторів телеграм-каналів, YouTube- та TikTok-сторінок тощо. Зазначено, що чинне законодавство не охоплює належним чином питання гарантій для неформалізованих журналістів, захисту джерел інформації, а також встановлення меж допустимого державного втручання в онлайн-комунікацію.

Окрему увагу приділено проблемі дезінформації, яка, попри свою небезпеку в умовах війни, не має в Україні чіткого законодавчого визначення. Розглянуто ризики свавільного обмеження свободи слова під виглядом боротьби з фейками, а також загрозу політично мотивованої онлайн-цензури за відсутності процесуального регулювання та ефективного судового контролю.

У дослідженні акцентовано на вразливості цифрової інфраструктури медіа до кібератак, технічного блокування та втручання, що становить загрозу як для свободи слова, так і для інформаційної безпеки. Обґрунтовано необхідність формування цілісного адміністративно-правового механізму цифрової безпеки, координації між державними органами, ЗМІ та цифровими провайдерами.

Наголошено також на важливості цифрової грамотності населення як умови усвідомленої реалізації права на свободу вираження поглядів. Запропоновано впровадження державних програм з медіаосвіти та інформаційної гігієни.

У підсумку зроблено висновок про необхідність розробки нових адміністративно-правових інструментів, які забезпечуватимуть баланс між захистом національної інформаційної безпеки та дотриманням міжнародних стандартів у сфері прав людини, зокрема свободи слова в цифрову епоху.

Ключові слова: свобода слова; цифровізація; адміністративно-правове регулювання; дезінформація; онлайн-цензура; інформаційна безпека; цифрові медіа; генеративний штучний інтелект; персональні дані; кіберзагрози; медіаграмотність; міжнародні стандарти.

Вступ. Цифровізація суспільства радикально трансформує традиційні механізми комунікації, доступу до інформації та реалізації фундаментальних прав і свобод людини. Особливого значення в цьому контексті набуває право на свободу слова, яке, з одного боку, значно розширює свої можливості через використання цифрових технологій, а з іншого, стикається з новими загрозами та обмеженнями,

зумовленими як технічними, так і нормативно-правовими чинниками. В умовах збройної агресії проти України проблема забезпечення свободи вираження поглядів в онлайн-просторі постає не лише як правозахисний, а й як елемент національної безпеки.

Сучасні виклики, зокрема поширення дезінформації, розвиток генеративного штучного інтелекту, уразливість цифрової інфраструк-

тури та зростання випадків політично мотивованого блокування інформаційних ресурсів, актуалізують необхідність переосмислення адміністративно-правових механізмів регулювання у цій сфері. Національне законодавство, попри прогрес у формуванні базових інститутів цифрового правопорядку, поки що не забезпечує належного рівня правової визначеності, узгодженості з міжнародними стандартами та ефективності у реагуванні на новітні загрози.

Постановка завдання. Метою цієї статті є комплексне дослідження основних адміністративно-правових викликів у сфері забезпечення свободи слова в цифрову епоху, аналіз чинної нормативної бази України, виявлення прогалин у регулюванні та розроблення пропозицій щодо вдосконалення відповідного правового механізму з урахуванням потреб демократичного розвитку, вимог безпеки та міжнародно-правових зобов'язань держави.

Методологія даної публікації ґрунтується на комплексі загальнонаукових та спеціально-юридичних методів. Формально-юридичний метод використано для аналізу норм національного та міжнародного законодавства у сфері свободи слова, цифрової безпеки й персональних даних. За допомогою логіко-семантичного підходу уточнено зміст ключових понять: «дезінформація», «онлайн-цензура», «цифрова грамотність» тощо.

Порівняльно-правовий метод дозволив зіставити українське регулювання з міжнародними стандартами. Системний аналіз застосовано для виявлення прогалин у правозастосуванні та визначення потреби в оновленні адміністративно-правових механізмів. Емпіричну базу становлять акти національного законодавства, міжнародні документи, судова практика та аналітичні звіти правозахисних організацій.

Результати дослідження. Цифровізація медіапростору в Україні зумовила глибинні трансформації у сфері реалізації свободи слова, водночас породивши нові адміністративно-правові виклики. Зокрема, йдеться про потребу нормативного визначення правового статусу цифрових платформ та розробки ефективних механізмів державного контролю, що не порушують засадничих прав людини.

Особливої актуальності набуває проблема балансу між свободою слова та національною безпекою в умовах інформаційної війни. Конституція України гарантує право на свободу думки і слова, однак допускає його обмеження в інтересах національної безпеки, громадського

порядку, що породжує практичні питання щодо доцільності та пропорційності відповідних обмежень.

В українському законодавстві відсутній нормативно-правовий акт, який би регламентував свободу слова в Інтернеті. Норми розосереджені між законами «Про інформацію», «Про медіа», «Про електронні комунікації», «Про захист персональних даних», але вони не охоплюють усього спектра викликів цифрового середовища: діяльність онлайн-платформ, блогів, соціальних мереж, анонімних каналів тощо. Внаслідок цього виникає правова невизначеність щодо регулювання інтернет-контенту, меж державного втручання, відповідальності за дезінформацію та гарантій для користувачів та журналістів.

Варто зауважити, що ухвалення Закону України «Про медіа» [1] стало важливим кроком до систематизації відповідної галузі. Закон вперше закріпив поняття онлайн-медіа та механізм їхньої добровільної реєстрації. Водночас низький рівень такої реєстрації обмежує можливість застосування гарантій до незареєстрованих суб'єктів, які де-факто виконують журналістські функції. Це позбавляє їх захисту в межах кримінального та кримінального процесуального законодавства, зокрема у контексті ст. 171 КК України, що ускладнює кваліфікацію правопорушень і обмежує юридичний захист.

Одним із головних викликів адміністративно-правового регулювання свободи слова в умовах цифровізації є відсутність визначеного правового статусу для більшості цифрових платформ і контент-мейкерів – блогерів, адміністраторів телеграм-каналів, YouTube- і TikTok-сторінок. Попри передбачену Законом України «Про медіа» можливість добровільної реєстрації онлайн-медіа, значна частина таких ресурсів функціонує поза межами правового поля.

Відповідні фактори ускладнюють реалізацію права на захист джерел інформації – фундаментального елементу свободи слова, визнаного міжнародними стандартами. В Україні це право поширюється переважно на журналістів зі визнаним статусом, у той час як автори неформалізованих онлайн-ресурсів залишаються без належного захисту.

Невизначеність правового статусу також створює проблеми у притягненні до відповідальності за порушення інформаційного законодавства. Ідентифікація винних осіб, встановлення зв'язку між контентом і його автором, а також

застосування адміністративних санкцій є наразі вкрай ускладненими. У результаті традиційні ЗМІ підлягають суворому регулюванню, тоді як цифрові платформи часто залишаються поза юрисдикцією державного контролю [2, с. 19].

Проблема загострюється в умовах воєнного стану та інформаційної агресії: анонімні цифрові платформи можуть використовуватись для деструктивних інформаційних впливів. Відсутність належного правового інструментарію не дозволяє державі оперативно реагувати без порушення основоположних прав.

Формування чіткого правового статусу онлайн-медіа та цифрових «контентотворців» є передумовою ефективного правозастосування. Адміністративно-правове регулювання повинно враховувати різноманіття цифрових форматів, рівень впливу ресурсу, характер і обсяг поширеного контенту. Водночас держава зобов'язана зберегти баланс між регуляцією та гарантіями свободи слова, включаючи захист джерел, доступ до публічної інформації та свободу журналістської діяльності [3, с. 15].

Таким чином, попри оновлення законодавства України у сфері медіа, залишаються системні правозастосовчі виклики. Фрагментарна імплементація Закону «Про медіа», відсутність чіткого захисту для неформалізованих журналістів та слабка практика у сфері охорони джерел інформації свідчать про потребу в комплексному удосконаленні адміністративно-правового механізму забезпечення свободи слова.

Як зазначає О. Петришин, виклики цифровізації полягають у необхідності формування нових моделей правового регулювання інформаційної сфери, які мають відповідати динаміці розвитку цифрових технологій, але при цьому не створювати надмірного втручання у свободу вираження поглядів [2, с. 20].

Контроль інформації в онлайн є одним із центральних викликів адміністративно-правового регулювання в умовах цифровізації. Поширення дезінформації стало критичною проблемою, особливо в умовах воєнного стану та інформаційної агресії з боку РФ. Попри відсутність законодавчого визначення терміна «дезінформація», чинне право передбачає відповідальність за недостовірні відомості, однак притягнення до відповідальності ускладнюється юридичною невизначеністю.

Українське законодавство не розрізняє види викривленої інформації (недостовірна, фейкова тощо), як це прийнято на міжнародному рівні. Відсутність правового визначення дезін-

формації унеможливлює ефективну протидію маніпулятивному контенту, особливо поширеному в соцмережах, месенджерах та анонімних каналах [4].

Право на спростування недостовірної інформації гарантується Конституцією та Цивільним кодексом України. Ст. 278 ЦКУ надає суду повноваження забороняти поширення шкідливої інформації, однак ці механізми є наслідковими, а не превентивними, й не встигають за динамікою цифрового середовища. Проблему ускладнює анонімність авторів контенту, іноземна юрисдикція тощо.

Закон України «Про медіа» [1] передбачає заходи регуляторного реагування (приписи, штрафи, вилучення з реєстру), проте вони застосовні лише до зареєстрованих суб'єктів, у той час як більшість дезінформаційного контенту продукується платформами поза наглядом регуляторів.

Однак доцільним вбачається всебічний аналіз зазначеної проблематики, з урахуванням в тому числі й протилежних підходів.

Так, в умовах воєнного стану питання допустимості обмеження інформації має вирішуватись із дотриманням принципів законності, чіткості правових процедур та неприпустимості запровадження прихованих форм цензури. В цьому питанні окрему загрозу становлять політично вмотивовані обмеження, що впроваджуються під виглядом протидії дезінформації, але фактично можуть призводити до звуження простору свободи слова.

Паралельно постає проблема онлайн-цензури. Попри конституційну заборону цензури та гарантії свободи слова, відсутність чітких процедур обмеження контенту створює ризики свавільного втручання. Органи державної влади (СБУ, Нацрада, ДССЗІ, Мінцифри) реалізують блокування ресурсів, проте їх дії часто залишаються непрозорими та позапроцесуальними – зокрема, через санкційні рішення РНБО.

Процедури блокування зазвичай не мають судового контролю, не забезпечують інформування власників ресурсів чи можливості оскарження, що суперечить стандартам ЄСПЛ (справи *Ahmet Yildirim v. Turkey*, *Cengiz and Others v. Turkey* тощо). У результаті втрачається межа між законною модерацією та репресивним втручанням, що створює стримуючий ефект на самовираження («chilling effect») [5].

Відсутність правового режиму онлайн-цензури загрожує як правам людини, так і національній безпеці. З одного боку, необхідно опера-

тивно реагувати на загрози, з іншого – уникати надмірної гнучкості правозастосування.

Розв'язання проблеми потребує встановлення прозорих процедур оцінки контенту, меж допустимого втручання, забезпечення судового або квазісудового контролю та реальних гарантій оскарження. Також необхідна системна інформаційна політика з формування критичного мислення, без чого правові заборони не забезпечать ефективної інформаційної безпеки.

Захист персональних даних та приватності в цифровому середовищі є одним з ключових компонентів адміністративно-правового регулювання свободи слова. Соціальні мережі й цифрові медіа активно обробляють персональні дані з метою таргетованої реклами, аналізу поведінки, персоналізації контенту, що створює ризики для інформаційної автономії особи. Застосування алгоритмів, мікротаргетингу та профілювання може обмежувати доступ до альтернативної інформації, формувати «інформаційні бульбашки» та приховано впливати на свідомість користувачів.

Незважаючи на те, що Закон України «Про захист персональних даних» [6] визначає основи правового регулювання, механізми контролю залишаються непослідовними, а санкції – малоефективними. Адміністративно-правове регулювання має охоплювати не лише безпеку даних, а й гарантувати недоторканність цифрового простору особи та свободу вираження.

Водночас, держава мусить дотримуватись балансу між заборонаю цензури та обов'язком захищати національну безпеку й інформаційний простір. Особливо це важливо під час війни, коли допустимість обмежень потребує законності, пропорційності та обґрунтованості. В умовах воєнного стану виникають ризики надмірної концентрації владних повноважень, зловживання блокуванням інформаційних ресурсів, підміни демократичного регулювання адміністративним втручанням. У таких умовах адміністративно-правовий механізм повинен не лише реалізовувати державну політику, а й стримувати потенційні зловживання [7].

Особливу актуальність набуває розвиток генеративного штучного інтелекту, здатного створювати текстовий, аудіо– та відеоконтент, що майже не відрізняється від створеного людиною. Найбільшу загрозу становлять deepfake-технології та автоматизоване продукування дезінформації, спрямованої на дестабі-

лізацію, дискредитацію держави та порушення етичних стандартів [3, с. 17].

Відповіддю має стати адаптація адміністративно-правового регулювання, зокрема: запровадження обов'язкового маркування ШІ-контенту; встановлення відповідальності за шкідливе використання ШІ у створенні дезінформації; створення механізмів верифікації джерел інформації, включаючи державне програмне забезпечення.

Генеративний ШІ вимагає нових, технологічно нейтральних правових інструментів, які забезпечуватимуть прозорість, відповідальність та інформаційну безпеку без необґрунтованого втручання в свободу вираження поглядів. Мета має залишатись ефективний захист суспільного інтересу в умовах демократичного правопорядку.

У цифрову епоху забезпечення цифрової безпеки стає основою адміністративно-правового захисту свободи слова. Вразливість журналістів, медіаорганізацій та активістів до кіберзагроз, технічного стеження й несанкціонованого доступу створює суттєві ризики, особливо в умовах війни. Незважаючи на існування нормативних актів («Про інформацію», «Про захист персональних даних», «Про основні засади забезпечення кібербезпеки України»), практична реалізація їх положень залишається недостатньо ефективною, а інституційна спроможність органів кіберзахисту обмеженою.

Станом на сьогодні в Україні відсутня єдина цілісна система цифрової безпеки. Повноваження між СБУ, Держспецзв'язком, Мінцифри та Нацполіцією часто дублюються та недостатньо координуються, що ускладнює запобігання кібератакам. Зростання атак на інформаційні ресурси, злами електронної пошти редакцій і правозахисників засвідчують системну вразливість медіаінфраструктури, яка є стратегічно важливою в умовах інформаційної війни [8, с. 38].

Особливу тривогу викликає ризик використання цифрових інструментів контролю з боку держави поза межами правового регулювання. Це ставить під загрозу права журналістів, конфіденційність джерел інформації та етичні стандарти. Адміністративно-правовий механізм повинен не лише захищати інформацію, а й гарантувати, що технологічні засоби не використовуються для обмеження свободи слова.

Вразливість інфраструктури медіа до кібератак, DDoS-ударів, блокувань серверів може призводити до повного паралічу ЗМІ, втрати

архівів і компрометації джерел. Особливо небезпечні цілеспрямовані втручання з боку іноземних структур, які прагнуть дестабілізувати незалежні медіа та створити інформаційний вакуум [8].

Посилює проблему відсутність належного технічного захисту в самих медіа, обмежені ресурси, недостатній рівень цифрової грамотності персоналу та слабка готовність державних органів до реагування. Особливо це критично у випадках транснаціональних атак або дій через інфраструктуру за межами юрисдикції України.

Таким чином, формування повноцінного адміністративно-правового механізму цифрової безпеки є необхідною умовою для захисту свободи слова у цифровому середовищі. Він має передбачати як інституційну координацію і реагування на кіберзагрози, так і гарантії недопущення зловживань під виглядом безпеки.

Однією з критичних загроз у цифровому середовищі є технічна ізоляція медіа, яка може здійснюватися як через блокування ресурсів за рішеннями державних органів чи в межах санкцій, так і шляхом обмежень з боку цифрових платформ – хостингів, соцмереж, реєстраторів доменів. За відсутності чітких правових процедур і можливості судового контролю такі дії можуть мати ознаки цензури та порушувати засади відкритості й плюралізму [9].

У цих умовах забезпечення цифрової стійкості медіа потребує ефективного адміністративно-правового регулювання, яке включає: розроблення стандартів кіберзахисту; впровадження механізмів реагування на кібератаки; підвищення цифрової компетентності працівників ЗМІ; створення системи координації між державою, медіа і цифровими провайдерами; гарантування прозорості обмежень доступу до інформації.

З огляду на масштаби цифрових ризиків, захист інформаційної інфраструктури медіа слід розглядати як компонент національної безпеки, що має здійснюватися з дотриманням принципів верховенства права і свободи вираження.

Низький рівень цифрової грамотності населення є ще одним суттєвим викликом для України. Відсутність навичок критичного аналізу джерел, розпізнавання дезінформації й маніпуляцій сприяє поширенню фейків, знижує якість публічного діалогу та підвищує вразливість населення до гібридних інформаційних впливів.

Адміністративно-правове регулювання

повинно враховувати потребу у формуванні цифрової компетентності громадян, адже ефективна протидія дезінформації неможлива без підготовленого інформаційного споживача. Інакше зростає нерівність у доступі до реалізації свободи слова через неспроможність брати участь у публічній комунікації [10].

Рекомендованими напрямами державної політики мають бути: державна підтримка програм медіаосвіти; освітні кампанії з цифрової безпеки; залучення громадських організацій до підвищення рівня медіаграмотності тощо.

Отже, цифрова освіта має розглядатися як необхідна умова реалізації свободи слова в цифрову епоху. Формальні гарантії залишаються недостатніми без свідомого, відповідального й захищеного поведіння з інформацією з боку кожного члена суспільства.

Ще одним із найбільш складних викликів для адміністративно-правового забезпечення свободи слова в Україні є суперечність між національними нормами та міжнародними стандартами, особливо в умовах воєнного стану. В епоху глобалізованого обміну інформацією гармонізація національного законодавства з міжнародними нормами у сфері цифрових прав стала не лише юридичною, а й політичною необхідністю.

Міжнародні акти – Міжнародний пакт про громадянські і політичні права (ст. 19), Європейська конвенція з прав людини (ст. 10) та практика ЄСПЛ – визначають чіткі критерії допустимості обмежень свободи вираження: вони мають бути законними, легітимними, необхідними у демократичному суспільстві та пропорційними.

В українській практиці цифрового регулювання ці принципи не завжди дотримуються. Зокрема, у період воєнного стану застосовуються блокування сайтів, санкційні обмеження, заборона доступу до платформ – часто без належної прозорості, правової визначеності або ефективного судового контролю. Це створює ризики конфлікту з міжнародними зобов'язаннями України та ускладнює інтеграцію до правового простору ЄС [8, с. 40].

В умовах збройної агресії держави-окупанта необхідність захисту інформаційної безпеки є очевидною, однак вона не повинна виправдовувати порушення принципів прав людини. Адміністративно-правовий механізм має забезпечувати, з одного боку, оперативне реагування на загрози, а з іншого – відповідність міжнародним стандартам, гарантії правової визначеності та тимчасовість обмежень.

Цифровізація медіапростору спричинила масштабні трансформації у сфері свободи слова. Вона відкрила нові канали для реалізації права на вираження поглядів, посилила доступ до інформації та розвиток громадянського суспільства, проте одночасно породила комплекс нових викликів для державного регулювання.

Серед головних адміністративно-правових викликів забезпечення свободи слова в цифрову епоху слід виділити наступні: неврегульованість статусу онлайн-медіа, кібервразливість інфраструктури, дезінформація та маніпулятивний контент (в тому числі й за допомогою ШІ), обмеженість захисту джерел інформації, низька цифрова грамотність громадян, а також розрив між національними і міжнародними підходами до свободи слова. Небезпеку також становить тенденція до надмірного втручання держави у медіапростір під приводом захисту безпеки.

Відповіддю на ці виклики має стати розробка оновлених адміністративно-правових інструментів, які забезпечуватимуть баланс між інформаційною безпекою та свободою вираження. Такий баланс повинен ґрунтуватися на принципах законності, пропорційності, підзвітності органів влади та відповідності європейським і міжнародним стандартам у сфері прав людини.

Висновки. Цифрова епоха трансформувала уявлення про свободу слова, водночас поставивши перед адміністративно-правовим регулюванням України низку складних викликів, що потребують комплексної та адаптивної відповіді з боку держави. Невизначеність правового статусу онлайн-платформ, зростання дезінформації, загрози кібератак, поширення технологій штучного інтелекту, обмежений захист джерел інформації та дефіцит цифрової грамотності населення – усе це формує нову конфігурацію правових ризиків, які не можуть бути ефективно вирішені інструментами традиційного адміністративного права.

У таких умовах забезпечення свободи слова потребує переосмислення механізмів регулювання з урахуванням принципів верховенства права, пропорційності та правової визначеності. Розробка нових адміністративно-правових інструментів має передбачати технологічну нейтральність, прозорість процедур, ефективний нагляд і контроль, а також інтеграцію міжнародних стандартів у національну практику. Лише на основі балансу між інформаційною безпекою та правами людини можна забезпечити стійкий розвиток медіасфери в умовах цифрової трансформації.

Список використаної літератури:

1. Про медіа: Закон України від 13 грудня 2022 р. № 2849-IX / Верховна Рада України. Відомості Верховної Ради України. 2023. № 47–50. Ст. 120. URL: <https://zakon.rada.gov.ua/laws/show/2849-20>.
2. Петришин О.В., Гиляка О.С. Права людини в цифрову епоху: виклики, загрози та перспективи. Вісник Академії правових наук України. 2021. № 1 (28). С. 17–27. DOI: 10.31359/1993-0909-2021-28-1-17.
3. Лисинюк М.В., Байда І.В. Трансформація культури медіаспоживання в умовах цифровізації суспільства. Вісник Національної академії керівних кадрів культури і мистецтв. 2024. № 2. С. 14–19. DOI: 10.32461/2226-3209.2.2024.308260.
4. Пропаганда та дезінформація: що найбільше впливає на український інфопростір [Електронний ресурс]. Національна спілка журналістів України. 2024. 25 грудня. URL: <https://nsju.org/novini/propaganda-ta-dezinformacziya-shho-najbilshe-vplyvaye-na-ukrayinskyj-infoprostir/>.
5. Кучин Т.Р., Костенко І.В. Свобода слова в епоху цифрових технологій: захист від цензури та онлайн-переслідувань. Науковий вісник Ужгородського національного університету. Серія: Право. 2024. Вип. 83. С. 121–125. DOI: <https://doi.org/10.24144/2307-3322.2024.83.1.18>. URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/07/20.pdf>.
6. Про захист персональних даних: Закон України від 1 червня 2010 р. № 2297-VI / Верховна Рада України. Відомості Верховної Ради України. 2010. № 34. Ст. 481. URL: <https://zakon.rada.gov.ua/laws/show/2297-17>.
7. Свобода слова під час війни [Електронний ресурс]. Національна рада України з питань телебачення і радіомовлення. 2024. 15 вересня. URL: <https://webportal.nrada.gov.ua/svoboda-slova-pid-chas-vijny/>.
8. Русавська А.О., Михайліна Т.В. Проблеми реалізації свободи слова в умовах збройної агресії. Право і суспільство. 2023. № 2. С. 38–43. DOI: 10.31558/2786-5835.2023.2.6.
9. Назарук В. Обмеження свободи слова під час війни: чи завжди вони виправдані [Електронний ресурс] / Вікторія Назарук. Четверта влада. 2023. 25 жовтня. URL: <https://4vlada.com/obmezhenia-svobody-slova-pid-chas-vijny-chy-zavzhdy-vony-vypravdani>.
10. Корецька В.О., Жебка В.В. Цифрова грамотність населення як фундамент цифровізації держави. Телекомунікаційні та інформаційні технології. 2022. № 3 (76). С. 12. DOI: 10.31673/2412-4338.2022.031220. URL: <https://tit.dut.edu.ua/index.php/telecommunication/article/view/2430/2311>.

Karapetyan O. O. Administrative and legal challenges to ensuring freedom of speech in the digital age

The article explores the contemporary administrative and legal challenges facing Ukraine in the process of ensuring freedom of speech amid the digitalization of the media space. The focus is placed on the transformation of traditional mechanisms of state regulation in the information sphere, driven by the rapid development of digital technologies, the expansion of social media functionalities, the emergence of generative artificial intelligence, and the intensification of security threats resulting from the armed aggression of the Russian Federation against Ukraine.

The study analyzes the absence of a comprehensive regulatory framework governing freedom of expression in the online environment, which leads to inconsistencies in law enforcement practices and legal uncertainty regarding the status of digital platforms, bloggers, administrators of Telegram channels, YouTube and TikTok pages, among others. It is emphasized that the current legislation does not sufficiently address the protection of informal journalists, the safeguarding of confidential sources, or the delineation of permissible state interference in online communication.

Particular attention is given to the issue of disinformation, which, despite its threat in wartime conditions, lacks a clear legal definition in Ukrainian law. The risks of arbitrary restrictions on freedom of expression under the guise of combating fake news, as well as politically motivated online censorship in the absence of procedural regulation and effective judicial oversight, are examined.

The article also highlights the vulnerability of digital media infrastructure to cyberattacks, technical interference, and targeted blocking, posing threats both to freedom of speech and to national information security. The necessity of developing a coherent administrative and legal framework for digital security is substantiated, including coordination among public authorities, media institutions, and digital service providers.

The importance of digital literacy among the population is underscored as a prerequisite for the conscious exercise of the right to freedom of expression. The implementation of national media education and information hygiene programs is proposed.

In conclusion, the article argues for the development of modern administrative and legal instruments that ensure a balance between protecting national information security and complying with international human rights standards, particularly those governing freedom of expression in the digital age.

Key words: *freedom of speech; digitalization; administrative and legal regulation; disinformation; online censorship; information security; digital media; generative artificial intelligence; personal data; cyber threats; media literacy; international standards.*