

**ОСОБЛИВОСТІ НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ
ВІДПОВІДАЛЬНОСТІ ЗА ПОРУШЕННЯ ПРАВИЛ ОХОРОНИ
ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ****FEATURES OF THE REGULATORY REGULATION OF LIABILITY FOR VIOLATION
OF THE RULES FOR THE PROTECTION OF TELECOMMUNICATIONS NETWORKS**

Актуальність статті полягає в тому, що питання охорони телекомунікаційних мереж набули особливого значення в умовах зростання кількості правопорушень, пов'язаних із пошкодженням кабельних ліній, незаконним втручанням у роботу електронних комунікаційних систем, самовільним підключенням до мереж, а також порушенням правил проведення робіт в охоронних зонах, такі дії не лише створюють технічні перешкоди у функціонуванні засобів зв'язку, а й можуть становити загрозу інформаційній безпеці держави, спричиняти порушення стабільності комунікацій та негативно впливати на забезпечення прав і свобод громадян. Наголошено, що застосування адміністративної відповідальності у сфері телекомунікацій має низку специфічних рис, зумовлених технічною складністю правопорушень, високою залежністю суспільства від електронних комунікацій та необхідністю оперативного реагування на будь-які порушення у роботі мереж. У цій сфері адміністративно-деліктні механізми виконують не лише каральну, а й превентивну функцію, спрямовану на забезпечення стабільності телекомунікаційної інфраструктури. З'ясовано, що міжнародні та європейські стандарти захисту телекомунікаційної інфраструктури формують важливу складову сучасної системи забезпечення інформаційної безпеки, оскільки встановлюють уніфіковані підходи до організації функціонування електронних комунікацій, захисту мереж від кібератак та забезпечення їх безперервної роботи. Умови глобальної цифровізації зумовили необхідність координації зусиль держав щодо протидії загрозам у кіберпросторі, що, своєю чергою, сприяло формуванню міжнародних правових і технічних стандартів у сфері телекомунікацій. Зроблено висновок про необхідність удосконалення механізмів притягнення до адміністративної відповідальності, зокрема шляхом уточнення складів правопорушень, підвищення рівня їх правової визначеності та адаптації до сучасних цифрових викликів. Особливої уваги потребує посилення відповідальності за посягання на об'єкти критичної телекомунікаційної інфраструктури, а також розвиток ефективних процедур фіксації та доказування правопорушень у цифровому середовищі. Також, доцільним вбачається систематизація адміністративно-правових норм у сфері електронних комунікацій, гармонізація національного законодавства з європейськими стандартами кібербезпеки, а також удосконалення взаємодії між регуляторними та правоохоронними органами. Перспективним напрямом також виступає впровадження сучасних технологічних засобів моніторингу стану телекомунікаційних мереж і цифрових інструментів фіксації правопорушень.

Ключові слова: телекомунікаційні мережі, електронні комунікації, суб'єкти господарювання, засади адміністративної відповідальності, адміністративно-правові норми, правове регулювання, органи державної влади.



The relevance of the article lies in the fact that the issues of protecting telecommunications networks have become particularly important in the context of an increase in the number of offenses related to damage to cable lines, illegal interference in the operation of electronic communications systems, unauthorized connection to networks, as well as violation of the rules for carrying out work in protected areas. Such actions not only create technical obstacles to the functioning of communications facilities, but can also pose a threat to the information security of the state, cause disruption of the stability of communications and negatively affect the protection of the rights and freedoms of citizens. It is emphasized that the application of administrative liability in the field of telecommunications has a number of specific features due to the technical complexity of offenses, the high dependence of society on electronic communications and the need for a prompt response to any violations in the operation of networks. In this area, administrative tort mechanisms perform not only a punitive, but also a preventive function aimed at ensuring the stability of the telecommunications infrastructure. It was found that international and European standards for the protection of telecommunications infrastructure form an important component of the modern information security system, as they establish unified approaches to organizing the functioning of electronic communications, protecting networks from cyberattacks and ensuring their uninterrupted operation. The conditions of global digitalization have necessitated the coordination of efforts of states to counter threats in cyberspace, which, in turn, contributed to the formation of international legal and technical standards in the field of telecommunications. The conclusion was made about the need to improve the mechanisms for bringing to administrative responsibility, in particular by clarifying the components of offenses, increasing the level of their legal certainty and adapting to modern digital challenges. Special attention is required to strengthen responsibility for encroachments on critical telecommunications infrastructure facilities, as well as the development of effective procedures for recording and proving offenses in the digital environment. It is also considered advisable to systematize administrative and legal norms in the field of electronic communications, harmonize national legislation with European cybersecurity standards, and improve interaction between regulatory and law enforcement agencies. A promising direction is also the introduction of modern technological means of monitoring the state of telecommunications networks and digital tools for recording offenses.

Key words: *telecommunications networks, electronic communications, business entities, principles of administrative responsibility, administrative and legal norms, legal regulation, state authorities.*

Актуальність теми. Особливого значення питання охорони телекомунікаційних мереж набули в умовах зростання кількості правопорушень, пов'язаних із пошкодженням кабельних ліній, незаконним втручанням у роботу електронних комунікаційних систем, самовільним підключенням до мереж, а також порушенням правил проведення робіт в охоронних зонах, такі дії не лише створюють технічні перешкоди у функціонуванні засобів зв'язку, а й можуть становити загрозу інформаційній безпеці держави, спричиняти порушення стабільності комунікацій та негативно впливати на забезпечення прав і свобод громадян.

Дослідження адміністративної відповідальності у сфері охорони телекомунікаційних мереж має важливе теоретичне та практичне значення, оскільки дозволяє визначити особливості правового регулювання відповідних суспільних відносин, виявити проблеми правозастосовної діяльності та сформулювати пропозиції щодо вдосконалення адміністративно-деліктного законодавства.

Виклад основного матеріалу. Особливість телекомунікаційних мереж як об'єкта адміністративно-правового захисту полягає у поєднанні матеріальної та інформаційної складових, до матеріальних елементів належать кабельні лінії, передавальні станції, серверне обладнання, технічні вузли та інші інженерні об'єкти. Водночас функціонування мереж забезпечує передачу інформаційних потоків, електронних даних і цифрових сигналів, які мають важливе значення для суспільства, держави та суб'єктів господарювання [1, с. 59–65]. Варто зазначити, що комплексний характер телекомунікаційних мереж обумовлює необхідність створення ефективного механізму їх адміністративно-правової охорони.

Зростання кількості загроз у сфері телекомунікацій обумовлює необхідність посилення державного контролю за функціонуванням мереж, удосконалення механізмів їх правового захисту та підвищення ефективності адміністративної відповідальності за порушення встановлених правил у сфері електронних комунікацій [2]. Надійний захист телекомунікаційної інфраструктури в сучасних умовах виступає важливою передумовою забезпечення інформаційної та національної безпеки України.

Нормативно-правове регулювання адміністративної відповідальності за порушення правил охорони телекомунікаційних мереж ґрунтується на системі законодавчих та підзаконних актів, які визначають порядок функціонування електронних комунікацій, встановлюють правила експлуатації телекомунікаційної інфраструктури та передбачають заходи юридичної відповідальності за їх порушення. Важливе місце у цій системі належить КУпАП, норми якого формують основу адміністративно-деліктного механізму захисту телекомунікаційних мереж.

КУпАП визначає загальні засади адміністративної відповідальності, поняття адміністративного правопорушення, види адміністративних стягнень, провадження у справах про адміністративні проступки. Своє відображення знаходять у положеннях КУпАП закріплено правові механізми реагування держави на порушення правил охорони телекомунікаційних мереж, незаконне втручання у функціонування засобів зв'язку та інші протиправні дії у сфері електронних комунікацій [3].

Особливе значення для дослідження адміністративної відповідальності у зазначеній сфері мають норми, які передбачають відповідальність за пошкодження ліній зв'язку, порушення правил їх охорони, самовільне проведення робіт в охоронних зонах телекомунікаційних мереж та недотримання встановлених технічних вимог. Вказані правопорушення створюють загрозу стабільності функціонування електронних комунікацій та можуть негативно впливати на інформаційну безпеку держави.

Аналіз положень КУпАП свідчить про те, що законодавець розглядає охорону телекомунікаційних мереж як важливий напрям адміністративно-правового захисту [3]. Наявність спеціальних складів адміністративних правопорушень у цій сфері дозволяє застосовувати заходи державного примусу до осіб, дії яких порушують нормальне функціонування телекомунікаційної інфраструктури. Одночасно чинне законодавство орієнтоване не лише на покарання винних осіб, а й на попередження нових правопорушень шляхом встановлення обов'язкових правил експлуатації та охорони мереж.

Разом із тим сучасний стан розвитку електронних комунікацій свідчить про необхідність подальшого вдосконалення положень КУпАП у відповідній сфері [3]. Поява нових технологій, зростання кількості кіберзагроз та зміна характеру правопорушень потребують оновлення окремих адміністративно-деліктних норм, уточнення складів правопорушень та посилення ефективності механізму притягнення до адміністративної відповідальності. Особливої актуальності такі питання набувають в умовах воєнного стану, коли стабільність функціонування телекомунікаційних мереж безпосередньо впливає на рівень інформаційної та національної безпеки України.

Важливе місце у системі нормативно-правового регулювання відносин у сфері електронних комунікацій займає ЗУ «Про електронні комунікації» [4], який визначає правові та організаційні засади функціонування телекомунікаційної інфраструктури, порядок надання електронних комунікаційних послуг, а також основні вимоги щодо забезпечення безпеки та стабільності функціонування мереж. Прийняття зазначеного Закону стало важливим етапом реформування національного законодавства у сфері зв'язку та його поступового наближення до європейських стандартів правового регулювання.

Положення Закону спрямовані на формування сучасної моделі регулювання електронних комунікацій, яка враховує розвиток цифрових технологій, потреби інформаційного суспільства та необхідність захисту інформаційного простору держави. Закон визначає правовий статус постачальників електронних комунікаційних мереж і послуг, встановлює вимоги до експлуатації технічних засобів, регламентує порядок доступу до інфраструктури та закріплює обов'язки суб'єктів у сфері електронних комунікацій щодо забезпечення цілісності та захищеності мереж.

Окрему увагу у Законі приділено питанням безпеки електронних комунікацій, зокрема, передбачено обов'язок операторів та постачальників послуг вживати необхідних технічних і організаційних заходів для мінімізації ризиків порушення функціонування мереж, запобігання несанкціонованому втручанням та забезпечення безперервності надання послуг зв'язку [4]. Подібні положення мають важливе значення для підтримання стабільності інформаційного простору держави та забезпечення належного рівня ІБ.

Нормативне регулювання у сфері електронних комунікацій не обмежується лише положеннями ЗУ «Про електронні комунікації» [4]. Значну роль відіграють також підзаконні нормативно-правові акти, які деталізують порядок функціонування телекомунікаційних мереж, визначають правила їх охорони, технічної експлуатації та взаємодії між суб'єктами у сфері зв'язку, до таких актів належать постанови Кабінет Міністрів України, нормативні документи центральних органів виконавчої влади, а також рішення Національної комісії, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку.

Особливе значення серед підзаконних актів мають правила охорони ліній електронних комунікацій, порядок проведення робіт у межах охоронних зон, технічні регламенти щодо експлуатації мереж та вимоги до захисту інформації. Визначальну роль відіграють зазначені нормативні документи визначають конкретні обов'язки фізичних та юридичних осіб у процесі використання телекомунікаційної інфраструктури та створюють правову основу для притягнення винних осіб до адміністративної відповідальності у разі порушення встановлених правил.

Сучасний розвиток цифрового середовища та зростання кількості загроз у сфері електронних комунікацій обумовлюють необхідність постійного оновлення нормативної бази. Удосконалення законодавства у цій сфері повинно бути спрямоване на підвищення рівня захисту телекомунікаційних мереж, забезпечення стійкості електронних комунікацій та адаптацію національного законодавства до міжнародних і європейських стандартів інформаційної безпеки.

Ефективність охорони телекомунікаційних мереж значною мірою залежить від належного функціонування системи державного контролю у сфері електронних комунікацій [5]. Контроль за дотриманням правил охорони мереж покладається на низку органів державної влади, компетенція яких визначається законодавством України та охоплює організаційні, наглядові, регуляторні й правоохоронні повноваження. Інтегрований багаторівневий механізм державного управління спрямований на забезпечення стабільного функціонування телекомунікаційної інфраструктури, запобігання правопорушенням та своєчасне реагування на випадки порушення встановлених правил.

Центральне місце у системі державного регулювання у сфері електронних комунікацій займає Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку. До її компетенції належить реалізація державної політики у відповідній сфері, здійснення регуляторних і контрольних функцій, прийняття нормативно-правових актів, а також контроль за дотриманням операторами та постачальниками електронних комунікаційних послуг вимог законодавства [6]. Комісія має право проводити перевірки, розглядати питання щодо порушення правил експлуатації мереж та застосовувати передбачені законом заходи реагування.

Важливу роль у забезпеченні охорони телекомунікаційних мереж відіграють також правоохоронні органи, насамперед Національна поліція України та Служба безпеки України, їх діяльність спрямована на виявлення, припинення та розслідування правопорушень, пов'язаних із пошкодженням телекомунікаційної інфраструктури, незаконним втручанням у роботу електронних комунікаційних систем, викраденням обладнання або здійсненням несанкціонованого доступу до мереж [7; 8]. Особливого значення діяльність зазначених органів набуває в умовах воєнного стану та зростання кількості кіберзагроз.

Окремі контрольні повноваження у сфері охорони телекомунікаційних мереж здійснюють органи місцевого самоврядування та місцеві державні адміністрації. У межах своєї компетенції вони беруть участь у погодженні проведення будівельних або земельних робіт, контролюють дотримання вимог щодо охоронних зон ліній зв'язку та взаємодіють з операторами електронних комунікацій у питаннях захисту об'єктів телекомунікаційної інфраструктури.

Значний обсяг контрольних функцій покладається також на органи, відповідальні за забезпечення кібербезпеки та захисту критичної інфраструктури, а їх діяльність пов'язана з моніторингом стану інформаційної безпеки, виявленням потенційних загроз для телекомунікаційних мереж та координацією заходів реагування у разі виникнення надзвичайних ситуацій або кібератак [9].

Наявність широкого кола суб'єктів державного контролю свідчить про комплексний характер охорони телекомунікаційних мереж. Водночас ефективність реалізації контрольних повноважень значною мірою залежить від належної координації діяльності органів державної влади, чіткого розмежування їх компетенцій та вдосконалення механізмів взаємодії у сфері забезпечення інформаційної безпеки держави.

Міжнародні та європейські стандарти захисту телекомунікаційної інфраструктури формують важливу складову сучасної системи забезпечення інформаційної безпеки, оскільки встановлюють уніфіковані підходи до організації функціонування електронних комунікацій, захисту мереж від кібератак та забезпечення їх безперервної роботи. Умови глобальної цифровізації зумовили необхідність координації зусиль держав щодо протидії загрозам у кіберпросторі, що, своєю чергою, сприяло формуванню міжнародних правових і технічних стандартів у сфері телекомунікацій.

Ключову роль у формуванні міжнародних стандартів відіграє ІТУ, який розробляє технічні рекомендації та нормативні документи щодо безпеки телекомунікаційних мереж, кіберстійкості інфраструктури та забезпечення надійності глобальних комунікаційних систем [9]. Документи ІТУ визначають базові принципи захисту мереж, включаючи вимоги до управління ризиками, захисту інформації та реагування на інциденти у сфері електронних комунікацій.

Важливе значення мають також стандарти, розроблені Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC), зокрема серія ISO/IEC 27000, яка регламентує систему управління інформаційною безпекою [10]. Чинні стандарти визначають комплексний підхід до захисту телекомунікаційних мереж, включаючи організаційні заходи, технічні засоби захисту, контроль доступу, криптографічні механізми та процедури реагування на кіберінциденти.

На європейському рівні значний вплив на формування стандартів захисту телекомунікаційної інфраструктури здійснює право ЄС. Зокрема, Директива NIS2 встановлює вимоги до кібербезпеки мережевих та інформаційних систем, визначає обов'язки операторів критичної інфраструктури щодо запобігання інцидентам і забезпечення стійкості цифрових сервісів. Директива передбачає посилений контроль за суб'єктами, які надають ЕКП, та запроваджує обов'язкові механізми повідомлення про кіберінциденти.

Окрім цього займають регламенти та рекомендації Європейського агентства з кібербезпеки (ENISA), яке здійснює аналітичну, методологічну та координаційну діяльність у сфері захисту інформаційної інфраструктури. Діяльність цього органу спрямована на підвищення рівня кіберстійкості телекомунікаційних мереж, розробку методичних рекомендацій для держав-членів ЄС та уніфікацію підходів до реагування на кіберзагрози.

Впровадження міжнародних та європейських стандартів у національне законодавство України має важливе значення для підвищення рівня захищеності телекомунікаційної інфраструктури [4]. Гармонізація правових норм сприяє удосконаленню системи кіберзахисту, посиленню стійкості електронних комунікаційних мереж та забезпеченню належного рівня ІБ держави в умовах зростання глобальних цифрових загроз.

Особливості кваліфікації правопорушень у цій сфері полягають у необхідності чіткого розмежування між пошкодженням, самовільним втручанням та незаконним використанням телекомунікаційних мереж [11]. Пошкодження передбачає фізичне або технічне порушення цілісності елементів інфраструктури, так самовільне втручання охоплює дії, спрямовані на зміну режиму роботи мереж без належного дозволу. Незаконне використання полягає у користуванні телекомунікаційними ресурсами без правових підстав або з порушенням встановлених правил. Правильна кваліфікація таких діянь має вирішальне значення для забезпечення ефективного застосування адміністративної відповідальності та захисту телекомунікаційної інфраструктури.

Порушення правил охорони телекомунікаційних мереж становлять різномірну за характером і наслідками сукупність протиправних діянь, які посягають на стабільність функціонування електронних комунікацій та безпеку інформаційного простору. Розмежування відповідних категорій дозволяє систематизувати типові випадки правопорушень, а також забезпечити більш точну кваліфікацію дій винних осіб та ефективне застосування адміністративної відповідальності.

Одним із найпоширеніших видів є пошкодження кабельних ліній та технічного обладнання, так порушення зазвичай виникають у процесі проведення будівельних, дорожніх або земляних робіт, коли не дотримуються встановлені вимоги щодо охоронних зон [12]. Пошкодження може мати як механічний характер (перерізання або руйнування кабелю), так і технічний (виведення з ладу обладнання), що призводить до перебоїв у роботі зв'язку та порушення доступу до телекомунікаційних послуг.

Окрім категорію становить несанкціоноване підключення до телекомунікаційних мереж. Подібні дії полягають у незаконному використанні ресурсів електронних комунікацій без дозволу оператора або постачальника послуг, а тому може проявлятися у самовільному підключенні до кабельних мереж, використанні чужої інфраструктури або отриманні доступу до послуг зв'язку

без належної оплати чи правових підстав. Згадані порушення не лише завдають економічної шкоди, а й можуть створювати додаткове навантаження на мережі та впливати на якість послуг.

Порушення правил проведення земельних або будівельних робіт у межах охоронних зон телекомунікаційних мереж є ще одним поширеним видом правопорушень [13]. У таких випадках суб'єкти господарювання або фізичні особи не дотримуються встановленого порядку погодження робіт, не враховують наявності підземних чи наземних комунікацій, що призводить до їх пошкодження, подібні дії свідчать про недостатній рівень організації робіт і порушення спеціальних вимог безпеки.

Важливе місце серед правопорушень займає втручання у функціонування мереж електронних комунікацій. Розглядаються дії, спрямовані на зміну режиму роботи мереж, блокування каналів зв'язку, несанкціоновану зміну налаштувань обладнання або вплив на передачу даних. Порушення можуть мати як умисний, так і необережний характер, однак у будь-якому випадку негативно впливають на стабільність телекомунікаційної інфраструктури.

Окремо слід виділити порушення режиму експлуатації технічних засобів зв'язку, так категорія охоплює недотримання встановлених технічних регламентів, правил обслуговування обладнання, умов його використання та зберігання [14]. Подібні порушення часто пов'язані з неналежною організацією роботи операторів або відповідальних осіб та можуть призводити до збоїв у роботі мереж або їх повного виходу з ладу.

У такий спосіб, види порушень правил охорони телекомунікаційних мереж відрізняються за способом вчинення, характером впливу на інфраструктуру та ступенем суспільної небезпеки. Комплексний аналіз відповідних явищ має важливе значення для вдосконалення правового регулювання у сфері електронних комунікацій та підвищення ефективності адміністративно-правового захисту телекомунікаційних мереж.

Застосування адміністративної відповідальності у сфері телекомунікацій має низку специфічних рис, зумовлених технічною складністю правопорушень, високою залежністю суспільства від електронних комунікацій та необхідністю оперативного реагування на будь-які порушення у роботі мереж. У цій сфері адміністративно-деліктні механізми виконують не лише каральну, а й превентивну функцію, спрямовану на забезпечення стабільності телекомунікаційної інфраструктури.

Порядок притягнення до адміністративної відповідальності регулюється положеннями КУпАП та спеціальними нормами законодавства у сфері електронних комунікацій [3]. Процедура починається з виявлення факту правопорушення, його фіксації уповноваженими органами, складання протоколу та подальшого розгляду справи компетентним органом або судом. Важливе значення має дотримання процесуальних гарантій осіб, які притягаються до відповідальності, зокрема права на захист, надання пояснень та оскарження прийнятого рішення.

Практика діяльності уповноважених органів свідчить про те, що у сфері телекомунікацій значну роль відіграють НКЕК, що здійснює державне регулювання у сфері електронних комунікацій, радіочастотного спектра та поштового зв'язку, а також правоохоронні органи. Регулятор забезпечує контроль за дотриманням правил експлуатації мереж та може застосовувати заходи адміністративного впливу до операторів і постачальників послуг. Правоохоронні органи, у свою чергу, здійснюють виявлення, припинення та документування правопорушень, особливо у випадках пошкодження інфраструктури або незаконного втручання у її роботу.

Співвідношення адміністративної, кримінальної та цивільно-правової відповідальності у сфері телекомунікацій визначається характером і ступенем суспільної небезпеки правопорушення. Адміністративна відповідальність застосовується у випадках менш тяжких порушень правил охорони мереж, що не спричинили значних наслідків [3]. Кримінальна відповідальність настає у разі умисного або особливо небезпечного втручання у роботу телекомунікаційних систем, яке призвело до істотної шкоди або загрози національній безпеці [15]. Цивільно-правова відповідальність, у свою чергу, пов'язана з відшкодуванням майнової шкоди, завданої внаслідок пошкодження або неправомірного використання телекомунікаційної інфраструктури [16].

Проведений аналіз свідчить, що чинний механізм адміністративно-правового реагування на порушення правил охорони телекомунікаційних мереж ще не забезпечує належного рівня ефективності в умовах сучасних цифрових викликів. На практиці виникають труднощі, пов'язані кваліфікацією окремих правопорушень, фіксацією цифрових доказів та з визначенням меж відповідальності між різними суб'єктами у сфері електронних комунікацій. Існуючі санкції не завжди відповідають ступеню суспільної небезпеки таких діянь, особливо у випадках посягання на об'єкти критичної телекомунікаційної інфраструктури [17]. Додатковим ускладнюючим

чинником виступає швидкий розвиток інформаційних технологій, який потребує постійного оновлення нормативно-правових механізмів захисту телекомунікаційних мереж та вдосконалення діяльності уповноважених органів.

Враховуючи наведене, система юридичної відповідальності у сфері телекомунікацій має комплексний характер та забезпечує різні рівні правового реагування залежно від тяжкості порушення, що дозволяє ефективно захищати та підтримувати стабільність телекомунікаційну інфраструктуру інформаційного простору держави.

Практика застосування адміністративної відповідальності у сфері охорони телекомунікаційних мереж демонструє наявність низки системних проблем, які ускладнюють ефективний правовий захист електронних комунікацій. Актуальні проблеми зумовлені як недосконалістю чинного законодавства, так і динамічним розвитком цифрових технологій, що випереджає нормативне регулювання [3].

Одним із ключових недоліків чинного адміністративного законодавства є фрагментарність правового регулювання у сфері охорони телекомунікаційної інфраструктури. Норми, які передбачають відповідальність за порушення правил охорони мереж, розосереджені в різних нормативно-правових актах і не завжди узгоджені між собою [17]. Такий стан речей створює труднощі у правозастосуванні, ускладнює кваліфікацію правопорушень та знижує рівень правової визначеності для суб'єктів господарювання і громадян.

Проблемним залишається також питання визначення складів адміністративних правопорушень у сфері телекомунікацій. У низці випадків законодавчі формулювання є надто загальними або оціночними, що ускладнює їх однозначне тлумачення. Відсутність чітких критеріїв розмежування між адміністративними проступками, кримінальними правопорушеннями цивільно-правовими деліктами призводить до неоднакової правозастосовної практики та знижує ефективність притягнення винних осіб до відповідальності.

Окрему увагу слід приділити необхідності посилення відповідальності за посягання на об'єкти критичної телекомунікаційної інфраструктури [18]. В умовах зростання кіберзагроз та воєнних викликів пошкодження або блокування телекомунікаційних мереж може мати наслідки загальнодержавного масштабу. У зв'язку з цим доцільним є перегляд санкцій за відповідні правопорушення, а також запровадження більш диференційованого підходу залежно від ступеня шкоди та характеру протиправних дій.

Важливим напрямом удосконалення правового регулювання гармонізація українського законодавства з правом Європейського Союзу. Особливе значення мають положення європейських директив у сфері кібербезпеки та електронних комунікацій, зокрема підходи до захисту критичної інфраструктури, управління кіберризиками та обов'язків операторів зв'язку щодо реагування на інциденти [19]. Адаптація національного законодавства до європейських стандартів сприятиме підвищенню рівня кіберстійкості телекомунікаційних мереж та інтеграції України до єдиного цифрового простору.

Серед основних пропозицій щодо вдосконалення механізму адміністративно-правового захисту телекомунікаційних мереж доцільно виділити необхідність систематизації норм адміністративного законодавства у цій сфері, уточнення складів адміністративних правопорушень із урахуванням сучасних технологічних реалій, запровадження чітких критеріїв розмежування видів юридичної відповідальності, а також посилення координації між регуляторними та правоохоронними органами. Окремо доцільно розвивати механізми цифрової фіксації правопорушень та використання електронних доказів у адміністративному провадженні.

Комплексне вирішення зазначених проблем дозволить підвищити ефективність адміністративно-правового захисту телекомунікаційної інфраструктури, забезпечити належний рівень інформаційної безпеки держави та створити більш стійку правову основу для функціонування електронних комунікацій в Україні.

У межах дослідження адміністративної відповідальності за порушення правил охорони телекомунікаційних мереж встановлено, що зазначена сфера характеризується підвищеною складністю правового регулювання та значною залежністю від технічного розвитку електронних комунікацій. Нормативна база, яка регламентує відповідні суспільні відносини, охоплює положення КУпАП, ЗУ «Про електронні комунікації» та значну кількість підзаконних актів, які деталізують правила експлуатації та охорони телекомунікаційної інфраструктури [3, 4]. Водночас виявлено наявність певних прогалин та колізій у правовому регулюванні, що ускладнює єдину та послідовну практику застосування норм.

Адміністративна відповідальність у сфері охорони телекомунікаційних мереж виконує важливу роль у забезпеченні стабільного функціонування електронних комунікацій [3]. Виступає одним із основних інструментів превенції правопорушень, сприяє дотриманню встановлених правил експлуатації мереж та забезпечує оперативне реагування держави на випадки їх пошкодження, самовільного втручання або незаконного використання [20]. У сукупності з іншими видами юридичної відповідальності адміністративно-правові заходи формують цілісну систему захисту телекомунікаційної інфраструктури, яка має стратегічне значення для інформаційної безпеки держави.

Висновки. Аналіз практичних аспектів правозастосування свідчить про необхідність удосконалення механізмів притягнення до адміністративної відповідальності, зокрема шляхом уточнення складів правопорушень, підвищення рівня їх правової визначеності та адаптації до сучасних цифрових викликів. Окремої уваги потребує посилення відповідальності за посягання на об'єкти критичної телекомунікаційної інфраструктури, а також розвиток ефективних процедур фіксації та доказування правопорушень у цифровому середовищі.

Також, доцільним вбачається систематизація адміністративно-правових норм у сфері електронних комунікацій, гармонізація національного законодавства з європейськими стандартами кібербезпеки, а також удосконалення взаємодії між регуляторними та правоохоронними органами. Перспективним напрямом також виступає впровадження сучасних технологічних засобів моніторингу стану телекомунікаційних мереж і цифрових інструментів фіксації правопорушень.

Список використаних джерел:

1. Головацький Н. Т. Способи і методи адміністративно-правового захисту персональних даних в мережі Інтернет: теоретичний аналіз та практичні аспекти. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2024. Вип. 84, ч. 3. С. 59–65. DOI: 10.24144/2307-3322.2024.84.3.9.
2. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV. URL: <https://zakon.rada.gov.ua/laws/show/3475-15>
3. Кодекс України про адміністративні правопорушення: Закон Української РСР від 07.12.1984 № 8073-X. URL: <https://zakon.rada.gov.ua/laws/show/80731-10>
4. Про електронні комунікації: Закон України від 16.01.2020 № 1089-IX. *Відомості Верховної Ради України*. 2021. № 12. Ст. 78. URL: <https://zakon.rada.gov.ua/laws/show/1089-20>.
5. Про Національну комісію, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку : Закон України від 16.12.2021 № 1971-IX. URL: <https://zakon.rada.gov.ua/laws/show/1971-20#Text>
6. Курус Т. В. Нормативно-правове регулювання електронного урядування в Україні. *Вісник Прикарпатського університету. Серія: Політологія*. 2024. Вип. 19. С. 63–70. DOI: 10.32782/2312-1815/2024-19-9.
7. Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII. URL: <https://zakon.rada.gov.ua/laws/show/580-19#Text>
8. Про Службу безпеки України : Закон України від 25.03.1992 № 2229-XII. URL: <https://zakon.rada.gov.ua/laws/show/2229-12#Text>
9. International Telecommunication Union. *Global Cybersecurity Index 2024*. Geneva : ITU, 2024. URL: <https://www.itu.int/epublications/publication/global-cybersecurity-index-2024/>
10. ISO/IEC 27001:2022. *Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. Geneva : International Organization for Standardization, 2022. URL: <https://www.iso.org/standard/27001>
11. Мазійчук В. А. Характеристика адміністративних правопорушень в інформаційній сфері. *Аналітично-порівняльне правознавство*. 2026. № 2. DOI: 10.24144/2788-6018.2026.02.2.27.
12. Про затвердження Правил охорони ліній електрозв'язку : Постанова Кабінету Міністрів України від 29.01.1996 № 135. URL: <https://zakon.rada.gov.ua/laws/show/135-96-%D0%BF#Text>
13. Земельний кодекс України : Закон України від 25.10.2001 № 2768-III. URL: <https://zakon.rada.gov.ua/laws/show/2768-14#Text>
14. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/1882-20>
15. Кримінальний кодекс України: Кодекс України; Закон від 05.04.2001 № 2341-III. База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/go/2341-14>

16. Шевчук М. О. Особливості правового забезпечення інформаційної безпеки з урахуванням сучасних загроз національній безпеці. *Правовий часопис Донбасу*. 2024. № 1 (86). С. 45–50. DOI: 10.32782/2523-4269-2024-86-45-50.

17. Туров В. Д. Використання інформаційних технологій на етапі доказування в адміністративному судочинстві України. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2024. Т. 2. Вип. 82. С. 283–288. DOI: 10.24144/2307-3322.2024.82.2.44.

18. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19>

19. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) (Text with EEA relevance). *Official Journal of the European Union*. 2018. L 321. P. 36–214. URL: <https://eur-lex.europa.eu/eli/dir/2018/1972/oj>

20. Цивільний кодекс України: Кодекс України; Закон від 16.01.2003 № 435-IV. База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/go/435-15>

Дата першого надходження статті до видання: 05.05.2026

Дата прийняття статті до друку після рецензування: 29.05.2026

Дата публікації (оприлюднення) статті: 15.06.2026