

# АДМІНІСТРАТИВНЕ ПРАВО І ПРОЦЕС; ФІНАНСОВЕ ПРАВО; ІНФОРМАЦІЙНЕ ПРАВО

УДК 342.9 (477)

DOI <https://doi.org/10.32782/pdu.2024.3.2>

**Д. В. Бондар**

кандидат наук з державного управління,  
ректор Львівського державного університету безпеки життєдіяльності  
ORCID: 0009-0004-9571-7828

## ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У СФЕРІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ: АДМІНІСТРАТИВНО-ПРАВОВІ ЗАСАДИ

Наукова публікація присвячена дослідженню адміністративно-правових засад використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності.

Зазначається, що сучасні досягнення науково-технічного прогресу мають значний потенціал щодо сприяння росту економіки, полегшення життя людини. Водночас різноманітні технічні засоби, комп'ютерні системи несуть з собою нові загрози життю та здоров'ю людини, адже не поодинокими є випадки несанкціонованого втручання в роботу вказаних систем, що призводить до техногенних аварій та навіть катастроф.

Акцентовано увагу на питанні адміністративно-правового врегулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, а саме, для запобігання виникненню надзвичайних ситуацій та подолання їх наслідків.

Здійснено аналіз чинного національного законодавства, яким врегульовано різні аспекти використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності.

Зазначається, що значну частину нагальних питань використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності слід вирішувати шляхом адміністративно-правового врегулювання відповідних суспільних відносин саме на рівні підзаконних (відомчих) нормативно-правових актів: наказів міністерств та інших центральних органів виконавчої влади.

Сформульовано висновок про те, що використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності доцільно врегульовувати спільними наказами Міністерства цифрової трансформації України та Міністерства внутрішніх справ України, що дозволить враховувати під час нормотворчої діяльності останні досягнення у сфері цифрових технологій. Також наголошується на необхідності детальної адміністративно-правової регламентації використання технології штучного інтелекту для запобігання виникненню надзвичайних ситуацій та подолання їх наслідків.

**Ключові слова:** інформаційні технології, адміністративно-правові засади, безпека життєдіяльності, надзвичайні ситуації, аварія, техногенна катастрофа, запобігання, правове регулювання, нормотворчість, запобігання.

**Актуальність теми.** Питання забезпечення безпеки життєдіяльності в сучасному світі набувають все більшої актуальності, адже розвиток високотехнологічного виробництва, поява технології штучного інтелекту та роботизованих систем вима-

гають особливої уваги до забезпечення безпеки людини та навколишнього середовища. Маючи значний потенціал щодо сприяння росту економіки, полегшення життя людини, різноманітні технічні засоби, комп'ютерні системи несуть із собою нові

загрози життю та здоров'ю людини, адже не поодинокими є випадки несанкціонованого втручання в роботу вказаних систем, що призводить до техногенних аварій та навіть катастроф. Більше того, досягнення науково-технічного прогресу часто умисно використовуються з протиправною метою або у військових цілях.

Вищевикладеним обґрунтовується необхідність належного правового врегулювання використання нових технологій з метою забезпечення безпеки життєдіяльності. Особливої уваги потребує питання адміністративно-правового врегулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, а саме, для запобігання виникненню надзвичайних ситуацій та подолання їх наслідків.

**Аналіз останніх досліджень і публікацій.** Правове регулювання використання інформаційних технологій у різних сферах суспільного життя досліджували такі відомі науковці як М. Бабик, Д. Біленька, О. Берназюк, М. Віхляєв, О. Гунбіна, К. Дубова, С. Єсімов, Т. Ковальова, Т. Коломоєць, О. Комаров, А. Комзюк, А. Краковська, І. Лопушинський, К. Оксютенко, А. Омельченко, М. Серебро, Р. Стефанчук, І. Тищенкова та інші.

Питанням забезпечення безпеки життєдіяльності присвятили свої роботи такі науковці як Ф. Апшай, О. Остапенко, О. Чекрыгін, О. Халак, О. Хитра та інші дослідники.

Проте, питання адміністративно-правових засад використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності ще не були предметом окремого наукового аналізу, чим обґрунтовується актуальність підготовки даної публікації.

**Постановка завдання.** Метою публікації є дослідження адміністративно-правових засад використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, що має створити підґрунтя для формування пропозицій щодо удосконалення чинного національного законодавства у даній сфері суспільних відносин.

Методологія даної публікації об'єднує три групи методів наукового пошуку:

філософські, загальнонаукові та спеціально-юридичні. Так, більшою мірою застосовуються закони та прийоми діалектики, системний та структурно-функціональний методи, прийоми логіки, формально-юридичний метод та метод юридичного моделювання. Крім того, використовуються загальновідомі наукові підходи: телеологічний, цивілізаційний, синергетичний тощо. Так, телеологічний підхід вимагає від дослідника не займатися наукою заради науки, адже кожне юридичне дослідження, кожна публікація на правову тематику повинні мати чітко визначену мету – сприяти удосконаленню чинного та формуванню перспективного національного законодавства, а також юридичної практики. Цивілізаційний підхід передбачає дослідження зарубіжного досвіду правового регулювання у тій або іншій сфері суспільних відносин із урахуванням національних правових традицій та звичаїв, адже кожна цивілізація має свій самобутній шлях розвитку і в процесі правових реформ необхідно враховувати особливості національної правосвідомості та правової культури, включаючи сферу правового регулювання безпеки життєдіяльності.

**Результати дослідження.** Сучасне суспільство справедливо називають інформаційним, виходячи із загального рівня цифровізації суспільних відносин та інтенсивного використання інформаційних технологій майже у всіх сферах суспільних відносин. Інформаційні технології дозволяють вирішувати значну частину актуальних питань, які виникають в повсякденній діяльності людини. Не останнє місце серед них займають питання забезпечення безпеки життєдіяльності.

Різноманітні технічні прилади, роботизовані системи, комп'ютери зі штучним інтелектом значно полегшують життя людини, проте зі збільшенням впливу техніки на суспільні відносини підвищується і рівень небезпеки, збільшується вірогідність техногенних аварій і катастроф. Особливої актуальності питання забезпечення безпеки життєдіяльності набуває в умовах ведення сучасних інформаційних війн, коли здійснюється несанкціоноване втручання в роботу інформаційних,

автоматизованих, електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, умисно розсилається шкідливе програмне забезпечення та спам. В таких випадках автоматизовані системи, які управляються комп'ютерами, замість виконання відпрацьованих функцій можуть завдати шкоду людині, майну, навколишньому природному середовищу.

Вищезазначене вимагає від органів публічної адміністрації здійснювати правове та організаційне забезпечення розробки та впровадження надійних систем захисту інформаційних ресурсів, інформаційно-комунікаційних систем та електронних комунікаційних мереж.

Крім того, актуальним напрямом нормотворчості є правове забезпечення використання інформаційних технологій для подолання наслідків надзвичайних ситуацій, виникненню яких сприяють техногенні аварії, катастрофи, епідемії, пожежі, стихійні лиха, використання військових засобів ураження, втручання в роботу інформаційних, роботизованих систем тощо.

До прикладу – інформаційні технології, включаючи електронні автоматизовані системи, можуть використовуватись для термінового оповіщення людей, блокування доступу до небезпечних об'єктів, автоматизованого використання засобів захисту, знезараження, забезпечення життєдіяльності в спеціалізованих укриттях тощо.

Таким чином, цифровізація суспільних відносин призводить до збільшення кількості потенційних загроз безпеці життєдіяльності людини і одночасно створює потужний інструментарій протидії негативним факторам, які порушують нормальні умови життя та діяльності людей на окремих територіях чи об'єктах.

Правильне застосування інформаційних технологій, тобто їх використання на користь суспільства та кожної людини, залежить від якості адміністративно-правового забезпечення процесів цифровізації та використання інформаційних технологій в певній сфері суспільних відносин. Саме органи публічної адміністрації створюють правила гри для учас-

ників визначених суспільних відносин, використовуючи класичні способи правового регулювання – дозволи, заборони та зобов'язання, а також такі традиційні методи правового регулювання як примус та заохочення (рекомендація).

Якщо у приватно-правовій сфері інформаційних відносин діє загально-дозвільний режим правового регулювання (дозволено все, що не заборонено законом), то в публічно-правовій сфері застосовується спеціально-дозвільний режим правового регулювання, згідно з яким дозволено лише те, що прямо передбачено законом.

Таким чином, використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності вимагає чіткої адміністративно-правової регламентації, адже суб'єкти владних повноважень не можуть діяти на власний розсуд, хоча і не позбавлені певних дискреційних повноважень.

Саме тому всі форми та способи використання інформаційних технологій, призначені для запобігання надзвичайним ситуаціям та ліквідації їх негативних наслідків, як правило закріплюються на рівні законів, постанов уряду, або оформлюються у вигляді певних інструкцій, порядків, положень та затверджуються наказами міністерств чи інших центральних органів виконавчої влади.

До прикладу – Положення про організацію оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та організації зв'язку у сфері цивільного захисту затверджено постановою Кабінету Міністрів України від 27 вересня 2017 р. № 733 [1].

Вказане Положення визначає порядок організації оповіщення органів виконавчої влади, органів місцевого самоврядування, підприємств, установ, організацій, органів управління і сил цивільного захисту та населення про загрозу виникнення або виникнення надзвичайних ситуацій, їх подальшого інформування з метою вжиття заходів безпеки, забезпечення зв'язком органів виконавчої влади та органів місцевого самоврядування у разі загрози виникнення або виникнення надзвичайних ситуацій та ліквідації їх наслідків,

а також забезпечення функціонування апаратури і технічних засобів оповіщення та технічних засобів електронних комунікацій. Дія цього Положення поширюється на центральні і місцеві органи виконавчої влади, органи місцевого самоврядування, операторів електронних комунікацій, аудіальні чи аудіовізуальні медіа, а також підприємства, установи, організації незалежно від форми власності і господарювання [1].

Правова регламентація використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності вимагає відповідної доктринальної основи, а саме наукового обґрунтування використання тих або інших способів та методів правового регулювання.

Крім того, питання використання інструментів цифровізації у сфері забезпечення безпеки життєдіяльності доцільно узгоджувати із профільним міністерством, яким наразі є Міністерство цифрової трансформації України.

Так, у відповідності до Положення про Міністерство цифрової трансформації України, затвердженого постановою Кабінету Міністрів України від 18 вересня 2019 р. № 856, Мінцифри є головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики: у сферах цифровізації, цифрового розвитку, цифрової економіки, цифрових інновацій та технологій, робототехніки та роботизації, електронного урядування та електронної демократії, розвитку інформаційного суспільства, інформатизації; у сфері впровадження електронного документообігу; у сфері розвитку цифрових навичок та цифрових прав громадян; у сферах відкритих даних, публічних електронних реєстрів, розвитку національних електронних інформаційних ресурсів та інтероперабельності, електронних комунікацій та радіочастотного спектра, розвитку інфраструктури широкопasmового доступу до Інтернету, електронної комерції та бізнесу; у сфері надання електронних та адміністративних послуг; у сферах електронної ідентифікації та електронних довірчих послуг; у сфері розвитку ІТ-індустрії; у сфері розвитку та функціонування

правового режиму Дія Сіті; у сфері хмарних послуг [2].

І саме Мінцифри відповідно до покладених на нього завдань координує діяльність міністерств, інших центральних органів виконавчої влади, Ради міністрів Автономної Республіки Крим, місцевих держадміністрацій, а також державних підприємств, установ, організацій та державних господарських об'єднань, навчальних закладів з питань, що належать до компетенції Мінцифри, надає їм необхідну методичну допомогу [2].

Таким чином, для адміністративно-правового регулювання питань, пов'язаних із використанням інформаційних технологій у сфері забезпечення безпеки життєдіяльності доцільно розробляти та видавати спільні накази Міністерства цифрової трансформації України та відповідного органу публічної адміністрації, який реалізує державну політику у вказаній сфері суспільних відносин.

Таким органом на даний час є Державна служба України з надзвичайних ситуацій.

Так, у відповідності до Положення про Державну службу України з надзвичайних ситуацій, затвердженого постановою Кабінету Міністрів України від 16 грудня 2015 р. № 1052, Державна служба України з надзвичайних ситуацій (ДСНС) є центральним органом виконавчої влади, діяльність якого спрямовується і координується Кабінетом Міністрів України через Міністра внутрішніх справ і який реалізує державну політику у сфері цивільного захисту, захисту населення і територій від надзвичайних ситуацій та запобігання їх виникненню, ліквідації наслідків надзвичайних ситуацій, рятувальної справи, гасіння пожеж, пожежної та техногенної безпеки, діяльності аварійно-рятувальних служб, а також гідрометеорологічної діяльності [3].

У відповідності до п. 4 вказаного Положення ДСНС відповідно до покладених на неї завдань узагальнює практику застосування законодавства з питань, що належать до її компетенції, розробляє пропозиції щодо вдосконалення законодавчих актів, актів Президента України, Кабінету Міністрів України, нормативно-правових актів міністерств та подає їх в установленому порядку Міністрові внутрішніх справ [3].

Таким чином, питання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності необхідно врегулювати спільними наказами Міністерства цифрової трансформації України та Міністерства внутрішніх справ України.

Проте, враховуючи важливість та особливу актуальність питання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, правове врегулювання відповідних суспільних відносин необхідно також здійснювати на рівні кодексів, законів, або принаймні на рівні постанов Кабінету Міністрів України.

Так, в Україні 1 липня 2013 року був введений в дію Кодекс цивільного захисту України, який регулює відносини, пов'язані із захистом населення, територій, навколишнього природного середовища та майна від надзвичайних ситуацій, пожеж та інших небезпечних подій, реагуванням на них, функціонуванням єдиної державної системи цивільного захисту, та визначає повноваження Кабінету Міністрів України, міністерств, інших центральних органів виконавчої влади, органів державної влади, що не входять до системи центральних органів виконавчої влади, Ради міністрів Автономної Республіки Крим, місцевих державних адміністрацій, органів місцевого самоврядування, встановлює права та обов'язки громадян України, іноземців та осіб без громадянства, підприємств, установ та організацій незалежно від форми власності (суб'єктів господарювання), а також інших юридичних осіб [4].

Крім того, в Україні розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р схвалено Концепцію розвитку штучного інтелекту в Україні.

У вказаній Концепції зазначено, що впровадження інформаційних технологій, частиною яких є технології штучного інтелекту, є невід'ємною складовою розвитку соціально-економічної, науково-технічної, оборонної, правової та іншої діяльності у сферах загальнодержавного значення. Відсутність концептуальних засад державної політики в галузі штучного інтелекту не дозволяє створювати та розвивати конкурентоспроможне середовище в зазначених сферах діяльності [5].

Враховуючи особливу роль кібербезпеки у сфері забезпечення безпеки життєдіяльності, основним завданням у сфері кібербезпеки під час реалізації державної політики розвитку галузі штучного інтелекту у вказаній Концепції названо захист комунікаційних, інформаційних та технологічних систем, інформаційних технологій, передусім тих, що використовуються операторами (постачальниками) ключових послуг (включаючи об'єкти критичної інфраструктури) і є важливими для безперервності функціонування держави, суспільства та безпеки громадян [5].

Причому для комплексного розв'язання проблем кібербезпеки Концепція розвитку штучного інтелекту в Україні, серед іншого, передбачає виконання такого завдання як удосконалення законодавства і створення сучасної нормативно-правової бази для впровадження кращих світових практик штучного інтелекту у сфері кібербезпеки і кіберзахисту [5].

Таким чином, саме на рівні кодексів та законів необхідно здійснювати правове врегулювання ключових питань використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, адже саме закон має вищу юридичну силу у порівнянні з відомчими (підзаконними) нормативно-правовими актами. Крім того, кодекси та закони характеризуються особливим порядком прийняття та внесення до них змін, що певною мірою гарантує стабільність в підходах до правового врегулювання тих або інших питань.

Водночас слід зазначити, що на рівні законів неможливо врегулювати всі аспекти використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, адже інформаційні відносини є вкрай мінливими. Крім того, цифрові технології розвиваються дуже активно, в короткі строки з'являються нові цифрові інструменти, що вимагає від органів публічної адміністрації оперативно реагувати на відповідні зміни та регламентувати використання останніх досягнень у сфері цифровізації.

Враховуючи вищевикладене, значну частину нагальних питань використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності слід

вирішувати шляхом адміністративно-правового врегулювання відповідних суспільних відносин саме на рівні підзаконних (відомчих) нормативно-правових актів: наказів міністерств та інших центральних органів виконавчої влади.

Важливе значення для адміністративно-правового врегулювання окремих питань використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності має нормотворча діяльність Президента України. До прикладу – це Концепція захисту населення і територій у разі загрози та виникнення надзвичайних ситуацій, схвалена Указом Президента України від 26 березня 1999 р. № 284/99 [6].

Так, у вказаній Концепції зазначається, що забезпечення захисту населення і територій у разі загрози та виникнення надзвичайних ситуацій, які згідно з класифікацією поділяються за характером на техногенні, природні, воєнні та соціально-політичні, а за рівнем – на загальнодержавні, регіональні, місцеві та об'єктові, є одним з найважливіших завдань держави. Актуальність проблеми забезпечення природно-техногенної безпеки населення і територій зумовлена тенденціями зростання втрат людей і шкоди територіям, що спричиняються небезпечними природними явищами, промисловими аваріями і катастрофами. Ризики надзвичайних ситуацій природного і техногенного характеру невпинно зростають. Забезпечення безпеки та захисту населення в Україні, об'єктів економіки і національного надбання держави від негативних наслідків надзвичайних ситуацій повинно розглядатися як невід'ємна частина державної політики національної безпеки і державного будівництва, як одна з найважливіших функцій центральних органів виконавчої влади, Ради міністрів Автономної Республіки Крим, місцевих державних адміністрацій, виконавчих органів рад [6].

До основних завдань захисту населення і територій під час надзвичайних ситуацій в Концепції захисту населення і територій у разі загрози та виникнення надзвичайних ситуацій віднесено, у тому числі: розроблення і реалізацію нормативно-правових актів, додержання державних технічних

норм та стандартів з питань забезпечення захисту населення і територій від наслідків надзвичайних ситуацій; збирання та аналітичне опрацювання інформації про надзвичайні ситуації; розроблення та забезпечення цільових і науково-технічних програм, спрямованих на запобігання надзвичайним ситуаціям та забезпечення сталого функціонування підприємств, установ, організацій незалежно від форм власності та підпорядкування, а також підвідомчих їм об'єктів виробничого і соціального призначення [6].

Отже, адміністративно-правова регламентація використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності є одним із пріоритетних напрямів державної політики.

З метою ефективного забезпечення безпеки життєдіяльності до основних заходів (інструментів) захисту населення і територій, які потребують правової регламентації слід віднести:

- автоматизовані системи оповіщення та інформування населення про надзвичайні ситуації, загрози безпеці життєдіяльності;

- автоматизовані системи спостереження та контролю за довкіллям, продуктами харчування, якістю води, повітря (включаючи хімічний та радіологічний контроль), інфраструктурою населених пунктів та іншими об'єктами з метою виявлення потенційних загроз безпеці життєдіяльності;

- автоматизовані системи обслуговування захисних споруд, сховищ та укриттів, підтримання їх в належному стані та забезпечення резервами продуктів харчування, води, повітря тощо;

- автоматизовані системи мобілізації людських та матеріально-технічних ресурсів, які необхідні для ліквідації наслідків надзвичайних ситуацій;

- автоматизовані системи забезпечення реалізації евакуаційних заходів: блокування та відкриття шляхопроводів, регулювання дорожнього руху, утворення додаткових шляхів евакуації (до прикладу – надувних сходів) тощо;

- автоматизовані системи протидії негативним чинникам, що сприяють виникненню надзвичайних ситуацій:

автоматизовані системи гасіння пожеж, знезараження (санітарної обробки, дезінфекції) об'єктів та територій тощо.

Наведений перелік автоматизованих систем цивільного захисту населення та забезпечення безпеки життєдіяльності не є вичерпним, адже сучасні інформаційні технології дозволяють вирішувати більшу частину складних завдань у вказаній сфері суспільних відносин без участі, але під контролем людини (оператора відповідної автоматизованої системи).

Формування повного структурованого переліку всіх можливих способів використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, а також обґрунтування необхідності адміністративно-правової регламентації кожного із зазначених способів, потребує проведення окремого доктринального дослідження.

**Висновки.** Проведене дослідження адміністративно-правових засад використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності дозволяє сформулювати висновок про те, що використання інформаційних технологій у вказаній сфері суспільних відносин доцільно врегульовувати на рівні кодексів та законів України, постанов Уряду та указів Президента України. Водночас нагальні питання доцільно врегульовувати спільними наказами Міністерства цифрової трансформації України та Міністерства внутрішніх справ України, що дозволить враховувати під час нормотворчої діяльності останні досягнення у сфері цифрових технологій.

Правової регламентації потребують, зокрема, конкретні напрями, способи та порядок використання автоматизованих систем у сфері забезпечення безпеки життєдіяльності, тобто систем, які управляються комп'ютером та спрацьовують автоматично, оперативно реагуючи на загрози безпеці життєдіяльності.

Крім того, об'єктивною є необхідність детальної адміністративно-правової регламентації використання технологій штучного інтелекту для запобігання виникненню надзвичайних ситуацій та подолання їх наслідків. Водночас загальні

питання та принципи використання технології штучного інтелекту у різних сферах суспільних відносин доцільно врегулювати на рівні окремого закону.

Необхідність формулювання конкретних пропозицій щодо внесення змін до чинного національного законодавства щодо врегулювання питання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності обумовлює перспективність подальшого дослідження даної теми.

### Список використаної літератури:

1. Про затвердження Положення про організацію оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та організації зв'язку у сфері цивільного захисту: постанова Кабінету Міністрів України від 27 вересня 2017 р. № 733. Дата оновлення: 13.03.2024. URL: <https://zakon.rada.gov.ua/laws/show/733-2017-%D0%BF#Text>
2. Положення про Міністерство цифрової трансформації України, затвердженого постановою Кабінету Міністрів України від 18 вересня 2019 р. № 856. Дата оновлення: 01.06.2024. URL: <https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#Text>
3. Положення про Державну службу України з надзвичайних ситуацій, затверджене постановою Кабінету Міністрів України від 16 грудня 2015 р. № 1052. Дата оновлення: 17.08.2024. URL: <https://zakon.rada.gov.ua/laws/show/1052-2015-p#Text>
4. Кодекс цивільного захисту України від 2 жовтня 2012 р. № 5403-VI. Дата оновлення: 21.09.2024. URL: <https://zakon.rada.gov.ua/laws/show/5403-17#Text>
5. Концепція розвитку штучного інтелекту в Україні, схвалена розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. Дата оновлення: 29.12.2021. URL: <https://zakon.rada.gov.ua/laws/show/1556-2020-p#Text>
6. Про Концепцію захисту населення і територій у разі загрози та виникнення надзвичайних ситуацій: Указ Президента України від 26 березня 1999 р. № 284/99. Дата оновлення: 26.03.1999. URL: <https://zakon.rada.gov.ua/laws/show/284/99#Text>

**Bondar D. Use of information technologies in the sphere of ensuring life safety: administrative and legal basis**

*The scientific publication is devoted to the study of the administrative and legal principles of the use of information technologies in the field of ensuring life safety.*

*It is noted that modern achievements of scientific and technological progress have significant potential for promoting economic growth and making human life easier. At the same time, various technical means and computer systems carry new threats to human life and health, because there are not infrequent cases of unauthorized interference in the operation of these systems, which leads to man-made accidents and even catastrophes.*

*The attention is focused on the issue of administrative and legal regulation of the use of information technologies in the field of ensuring life safety, namely, to prevent the occurrence of emergencies and overcome their consequences.*

*The current national legislation is analyzed, which regulates various aspects of the use of information technologies in the field of ensuring life safety.*

*It is noted that a significant part of the urgent issues of the use of information technologies in the field of ensuring life safety should be resolved through administrative and legal regulation of relevant social relations at the level of subordinate (departmental) regulatory legal acts: orders of ministries and other central executive bodies.*

*The conclusion is formulated that the use of information technologies in the field of ensuring life safety should be regulated by joint orders of the Ministry of Digital Transformation of Ukraine and the Ministry of Internal Affairs of Ukraine, which will allow taking into account the latest achievements in the field of digital technologies during regulatory activities. The need for detailed administrative and legal regulation of the use of artificial intelligence technology to prevent the occurrence of emergencies and overcome their consequences is also emphasized.*

**Key words:** *information technologies, administrative and legal principles, life safety, emergencies, accident, man-made disaster, prevention, legal regulation, rulemaking, prevention.*